RL-TR-92-329
Final Technical Report
December 1992

CENTRALIZED MAINTENANCE EVALUATION

Science Application International Corporation

Robert D. Lambert and David D. Sorensen

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

Rome Laboratory
Air Force Materiel Command
Griffiss Air Force Base, New York

This report has been reviewed by the Rome Laboratory Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RL-TR-92-329 has been reviewed and is approved for publication.

APPROVED: William R. Herrmann

WILLIAM R. HERRMANN
Project Engineer

FOR THE COMMANDER: Albert A. Jamberdino

ALBERT A. JAMBERDINO
Acting Technical Director
Directorate of Intelligence and Reconnaissance

If your address has changed or if you wish to be removed from the Rome Laboratory mailing list, or if the addressee is no longer employed by your organization, please notify RL(IRDW) Griffiss AFB, NY 13441-4114. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1992	Final Aug 91 - Sep 92

4. TITLE AND SUBTITLE
CENTRALIZED MAINTENANCE EVALUATION

5. FUNDING NUMBERS
C - F30602-91-D-0007
Task 8
PE - 31335F
PR - 2183
TA - QG
WU - 14

6. AUTHOR(S)
Robert D. Lambert and David D. Sorensen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Science Application International Corporation
803 West Broad Street
Falls Church VA 22046-3199

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Rome Laboratory (IRDW)
32 Hangar Road
Griffiss AFB NY 13441-4114

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
RL-TR-92-329

11. SUPPLEMENTARY NOTES
Rome Laboratory Project Engineer: William R. Herrmann/IRDW/(315)330-3127.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
This report documents the Centralized Maintenance Evaluation (CME). The CME was a project to demonstrate and evaluate the generic concept of operations, procedures, requirements, and responsibilities for centralized maintenance support for AN/GYQ-21 (V) Intelligence Data Handling Systems (IDHS). The report documents the technical work accomplished and the information gained during the performance of the CME task. The report includes observations, the nature of problems, positive and negative results, procedures followed, processes developed, and "lessons learned".

14. SUBJECT TERMS	15. NUMBER OF PAGES
Remote Computer Diagnostics; AN/GYQ-21(V); Intelligence Data Handling; Centralized Maintenance	76
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

TABLE OF CONTENTS

LIST OF FIGURES

TABLES

APPENDICES

FOREWORD

This Final Report was prepared entirely by Science Applications International Corporation under Task 8 of the Sterling IMD, KSC Operations' RL/IRD Task Ordering Agreement Contract F30602-91-D-0007.

1.0 INTRODUCTION

This is the final report for the Centralized Maintenance Evaluation (CME). The CME was a project to demonstrate and evaluate the generic concept of operations, procedures, requirements, and responsibilities for centralized maintenance support for AN/GYQ-21(V) Intelligence Data Handling Systems (IDHS). The project, which was accomplished between 1 August 1991 and 30 September 1992, was a natural developmental step toward the implementation of centralized maintenance using remote diagnostics (CM/RD) after previous studies determined the feasibility and cost-benefit tradeoffs for remote diagnostics.

1.1. Purpose

This report documents the technical work accomplished and the information gained during the performance of the CME task. The report includes observations, the nature of problems, positive and negative results, procedures followed, processes developed, and "lessons learned."

1.2. Background

In the fall of 1990, the United States Air Force Intelligence Support Agency (AFISA), Directorate of Intelligence Systems (IND) and the Warner Robins Air Logistics Center (WR-ALC) Single Service Logistics Support Manager (SSLSM) began exploring techniques to reduce maintenance costs associated with the AN/GYQ-21(V) IDHS and AN/GYQ-50(V) Intelligence Host Processing Systems (IHPS). They needed to find a method of containing maintenance costs while maintaining system effectiveness in the current and future environments of sharply reduced Department of Defense (DoD) budgets and funding. The application of remote diagnostic support was seen as a possible method to accomplish this goal. Science Applications International Corporation (SAIC) conducted research into alternative maintenance solutions during the Spring and Summer of 1991. The results of the research were published in a series of documents (see Appendix B for a list of relevant documents) leading to the ***Final Report on Remote Diagnostics***. SAIC concluded that remote diagnostic systems can provide a feasible and cost-effective maintenance support tool. However, the concept needed to be demonstrated and evaluated in the unique security environment of the Department of Defense Intelligence Information System (DoDIIS) community. As a result, the CME project was established.

During the CME, the Hercules Secure Remote Diagnostic Service ("Hercules"), a system of remote diagnostic services that has been successfully used by the National Security Agency (NSA) for over 10 years, was to be demonstrated and evaluated at one or more IDHS sites. The sites chosen typified Service (U.S. Army, U.S. Navy, and U.S. Air Force) implementations, as well as Joint Service implementations of CM/RD concepts. By choosing a site from each of the Services, the Government would be able to determine and to address both the common and the Service-unique security and communications issues for a representative set of IDHS sites. It was hoped that implementation of the CM/RD concept could be accelerated by addressing and solving security and communications problems during the CME.

The first site at which the CME was to be accomplished was the Rome Laboratory Intelligence Information Processing Facility (IIPF). The IIPF provided an environment where remote diagnostic services could be evaluated without affecting an operational site. The second site selected for the evaluation was the U.S. Army Foreign Science and Technology Center (FSTC), and the third site was a Joint Services site, the Joint Intelligence Center, Pacific (JICPAC). Concurrent with these evaluations, a fourth site was established at the AFISA Repair and Reconditioning Facility (the "Boneyard") to evaluate the Central Operation Remote Diagnostic System (CORDS), a prototype system developed by GTE for remote diagnosis of AN/GYQ-21(V) workstations and local area networks.

2.0 THE WORK PLAN AND FORMULATION OF THE RDWG (CDRL H003)

The Work Plan defined the project tasks and actions necessary for documenting the Centralized Maintenance Evaluation, the resulting implementation recommendations, and the implementation plan. The Work Plan proved to be a key document as it was the vehicle for coordinating and documenting considerable refinements to the planning used to generate the Statement of Work (SOW) for this task.

2.1. Findings

The significant issues associated with the Work Plan were as follows:

- The requirement for close coordination between many participants was identified. A CME Working Group (later renamed the Remote Diagnostics Working Group (RDWG)) was formed. Current membership is found in Appendix C. This group became the primary coordinating and action body for the task and was a very successful forum. Issues worked included:

  - Future maintenance and logistics concepts.
  - Communications requirements for remote diagnostics.
  - Security procedures for remote diagnostics.
  - Accreditation packages.

- The RDWG was very ambitious in its planning for the CME. They initially failed to appreciate the complexity of coordination necessary for this task. SAIC was able to illustrate several conflicts with the specific sequencing and scheduling of activities and deliverables found in the SOW. More realistic schedules were agreed upon and Government responsibilities that would allow the schedule to be met were identified. Table 1 and Table 2 in Appendix D present the schedule that was developed by the working group. While a close working relationship with SAIC and the success of the RDWG overcame several hurdles, the project required major re-directions during the period of performance (Table 3, Appendix D illustrates the resultant schedule revisions). As a result of the necessity to re-schedule activities, only one of the four site evaluations will be completed during the period of performance, and receipt of data from the evaluation will be too late to incorporate into the documentation as originally planned.

- The Government was forced to base the specifics of the SOW on contract and fiscal expenditure constraints rather than realistic requirements for services. This compounded the planning problem described above and resulted in additional mid-course corrections to permit useful support work to be accomplished in spite of the SOW rather than because of it.

- From the beginning, the Defense Intelligence Agency (DIA), a key decision-maker for information system security policy and procedures that would affect CME planning and procedures, chose not to participate in the RDWG.

- Most of the evaluation sites were firmly identified. The exception was the Navy site. Originally envisioned to be located at the Suitland, MD, facility, the site was later changed to JICPAC.

2.2. Lessons Learned

- CM/RD planning for the entire IDHS community is a volatile undertaking due to the extent of coordination. Tasking and planning need to be flexible and timelines must be realistically conservative.

- Within the DoDIIS community there are activities, organizations, and individuals with key go/no-go decision making power that is relevant to CM/RD implementation. All must participate in project planning.

- Staff representatives for communications and automated data processing (ADP), especially security specialists, need to be involved throughout the planning process.

- A good working team, such as the RDWG, can conduct planning rapidly and can review proposed plans and procedures quickly if the plans and procedures are developed and presented in an evolutionary manner. A working group, with key decision-makers as members, is the most effective forum for rapid action.

- Scheduled activity at a particular IDHS site may change unpredictably, thereby impacting CM/RD planning and implementation. Changing mission support requirements and contract deliverables may likewise impact schedules.

3.0 GENERAL EVALUATION PLAN (CDRL H004)

The General Evaluation Plan documented the generic concept of operations, procedures, requirements, and responsibilities for evaluating a concept of centralized maintenance for AN/GYQ-21(V) IDHS. Site-specific evaluation procedures were developed separately and attached as Annexes to the General Evaluation Plan as they were completed. (The site-specific plans are described in section 4.0 of this report.) The General Evaluation Plan described the three basic concepts of operation to be considered:

- Selected On-call Remote Diagnostics.
- Partial Remote Diagnostics.
- Full Remote Diagnostics.

Concepts for using the two CM/RD systems to be evaluated, Hercules and CORDS, and the known evaluation sites were described. A Navy site had not yet been identified by the Government. The responsibilities and requirements for each category of participants were described, concentrating on the areas of hardware, software, security, communications, and data collection. Responsibilities of specific participants were also identified within these descriptions. Both Government and contractor responsibilities were included. Evaluation criteria were matched against each category of CM/RD service to be provided by Hercules and CORDS. Technical and operational data collection objectives, which expanded on the criteria, were listed. The methods and procedures for logging and collecting data at both service centers and sites were identified. A CME Data Collection Form was included as an annex. SAIC described how we would analyze and report findings. Finally, planned evaluation sequencing, dates, and projected time "windows" were included as a schedule of events.

4.0 SITE SPECIFIC SCENARIOS AND PROCEDURES (CDRL H005)

The three annexes to the General Evaluation Plan were to be completed approximately two weeks prior to the specific site evaluation. Only the Rome Laboratory (RL) IIPF (Annex D) and the "Boneyard" (Annex E) scenarios and procedures were published in a final version, as the Army and Navy site evaluations, which were to follow the RL evaluation, never approached the two-week time frame for delivery called for in the SOW. However, considerable preparation for the Army and Navy site evaluations was accomplished. Initial and follow-up site surveys were completed for FSTC, and an initial site survey was completed for JICPAC. Draft scenarios and procedures were developed for both the FSTC and JICPAC sites.

The site-specific plans documented the concepts of operations for CM/RD and for performing the evaluations. They identified the IDHS equipment to be evaluated, their specific locations, and the connectivity to diagnostic and communications equipment. The conditions for help-desk and computer-to-computer operations were clearly specified and security constraints described, as were procedures for activating each service.

The plans provided detailed scenarios for evaluating several types of failures: normal, induced, and scripted (in the event insufficient actual failures occurred for full evaluation). The evaluations were to be managed as a series of tasks. These were described down to individual equipment levels. The tasks were as follows:

- Pre-evaluation Site Set-up was to be a one-week period to install, check-out, and correct discrepancies in equipment and procedures.

- Preventive Maintenance actions would be run against each major piece of IDHS equipment by the Hercules service.

- Remedial Maintenance would use pre-faulted modules to exercise the Hercules system. If time permitted, scripted failures and any actual hardware failures that occurred during the CME would be evaluated.

- General Technical Support evaluations would collect information on a variety of technical support tasks provided as part of the Hercules service.

- Software Transfer capabilities from the Hercules center would be evaluated using unclassified software. This task would demonstrate and evaluate the capability to upgrade or correct software from a central maintenance facility.

- Final Preventive Maintenance would be performed to ensure the site IDHS was left in good running condition following the evaluation.

The specific requirements for hardware, hardware modification, software, software modification, security, and communications were described for each site. Specific responsibilities for each participant at the site, Hercules center, and supporting locations were listed.

The approaches, findings, problems, and lessons learned below were based on issues identified during the planning process. No actual evaluations had been conducted at the time of this report and, therefore, no feedback on the strengths or weaknesses of the plans was available.

4.1. Rome Laboratory Intelligence Information Processing Facility

The first site at which the CME was to be accomplished was the RL IIPF. By using the IIPF as the first site, we could evaluate the remote diagnostic service in a controlled IDHS test bed environment while not affecting an operational site. The RL evaluation was originally scheduled for December 1991, but it was repeatedly delayed until September 1992 due to difficulties in determining and meeting DIA conditions for security. Additional delays were encountered due to schedule conflicts with other activities at the IIPF and the Hercules center. And a last minute one-week delay was called for when Hercules technicians encountered an unexpected hardware problem involving Hercules to STU-III connectivity. On-site activities for the evaluation finally began 16 September 1992 and concluded 25 September 1992 after successfully demonstrating the concept.

Three typical AN/GYQ-21(V) systems were chosen for evaluation. These were a VAX 11/785 Computer-Aided Tactical Information System (CATIS), a PDP 11/84 Communications Support Processor (CSP), and a Digital Equipment Corporation (DEC) 5000 workstation. For complete security during the evaluation, no classified data would be present on the systems, and only unclassified error register diagnostic data would be transmitted between the IIPF and the Hercules center. Computer-to-computer diagnostic access to the IIPF systems would be strictly controlled by IIPF personnel.

GTE technicians identified hardware modules that corresponded with the evaluation objectives for each system. GTE then obtained these modules configured with known faults (pre-faulted). Before using the pre-faulted modules in this evaluation, local GTE technicians verified the faults by installing the modules on equipment at the Boneyard and cross-checking the faults using CORDS or other diagnostic aids.

4.1.1. Findings

- Special and redundant procedures were required to ensure that security policy and procedures were followed during the evaluations. Even with the redundancy and detailed procedures, participants in the evaluation had difficulty understanding the extent of the communication security and computer security being provided.

- Setup of the evaluation took approximately three days to allow for installing the hardware and software, establishing the communications link, and pre-testing the operational and security procedures.

- In May 1992, DIA provided conditional approval to proceed with the evaluation. They had three conditions: (1) RL must formally request approval to connect the IIPF to Hercules; (2) No classified data could be contained in the systems while linked to Hercules; and (3) DIA would be provided a copy of the evaluation results. DIA would review the results prior to approving evaluations at other sites.

- The available technical documentation for the AT&T secure telephone unit (STU-III) was inadequate (see paragraph 4.1.2).

- Data and information from the Hercules center indicate that the projected use of CM/RD for computer-to-computer data communications is infrequent enough that it is not cost-effective to use a dedicated circuit.

4.1.2. Problems

- The delay of the RL evaluation until September 1992 was due to the following:

  1) A lack of DIA policy and procedures for the use of STU-IIIs in a CM/RD environment. No dedicated secure communications existed between the IIPF and Hercules, leaving STU-IIIs as the only available method.
  2) The length of time to develop the DIA policy and procedures.
  3) The length of time to obtain DIA approval to proceed with the evaluation.
  4) The length of time to develop NSA STU-III procedures for Hercules (based on DIA policies, procedures, and approval).
  5) Technical check-out of Hercules/STU-III communications.

- The development of pertinent policies and procedures were impacted by the reorganization activities at DIA and the Defense Information Systems Agency (DISA) as their new information system responsibilities and roles were, and still are, being defined and redefined.

- Government coordination of the formal request to connect the IIPF to Hercules took longer than the Government expected.

- An additional one week delay was incurred because the Hercules system could not communicate through the AT&T STU-III data port. Hercules engineers delayed testing the Hercules/STU-III configuration until after NSA approved the use of STU-IIIs. When they began testing the connectivity, they found that the available technical documentation for the STU-III did not adequately identify the required data port configurations. After directly discussing the problem with AT&T engineers, the Hercules engineers were able to make the necessary modifications to Hercules equipment, cables, and connectors.

- CATIS testing at the RL IIPF also impacted scheduling of the CME.

4.1.3. Lessons Learned

- DIA participation in planning for the CME and future related activities is essential. The reluctance of DIA to participate in the CME caused continual coordination delays, re-planning, and rescheduling of the evaluations. Additionally, DIA must review the results of the RL evaluation in order to determine if the security procedures for the CME were adequate. As DIA becomes better acquainted with and more involved with the concepts and planning for remote diagnostic support, DIA's approval for follow-on evaluations and subsequent installations should be easier to obtain.

- There appears to be a fairly standard set of paperwork that needs to be submitted and processes that need to be followed. The accreditation packages and approval processes that were developed for the RL will serve as a baseline example for other evaluation sites. As more and more operations are approved, submission of the approval packages should become even more standardized, and the time required for the process should shorten.

- Initial implementations of CM/RD communication and computer security features will be subject to human misunderstanding until these features and associated procedures have been operational for some period of time. Special effort must be given to education and monitoring the procedures and processes during this time to ensure full and early understanding of the technical and procedural issues associated with communication security and computer security relative to CM/RD.

- A long lead time is required for coordination among Government agencies, and for the determination of policies and procedures used in the evaluation of new concepts. While a working group can speed these processes considerably, there is still formal coordination that cannot be resolved through a working group forum.

- CM/RD use of secure lines should be shared with other uses of the secure communications.

4.2. AFISA AN/GYQ-21(V) Repair and Reconditioning Facility ("Boneyard")

Unlike the other evaluations, the Boneyard evaluation was specifically designed to demonstrate the capabilities of CORDS, and to determine if it can be successfully implemented to support IDHS hardware maintenance. The Boneyard evaluation was initially to have been conducted starting in December 1991 and continuing through the end of March 1992. This evaluation was to run longer than the other evaluations as this would permit a wider range of variables to be tested. The Boneyard evaluation involved only unclassified equipment, facilities, and data, and was unconstrained by the security restrictions that affected the planning and accomplishment of the other evaluations. Delays due to higher priority tasks and system problems prevented any evaluations during the original scheduled times. Higher priority tasks continued to take precedence. At the time this report was published, the CORDS evaluation was still being delayed.

Although CORDS was originally designed to support a series of workstations and small mini-computers or MicroVAX systems, the evaluation would also explore possible capabilities to support VAX 11/785, PDP 11/70, and IBM 4381 equipment. The Government could elect to evaluate CORDS for any IDHS that cycled through the Boneyard during the extended evaluation period. The evaluation was to occur in two phases. During the first phase, CORDS would be located at the Boneyard and linked to equipment by a null-modem or modem-to-modem connection. In the second phase, CORDS would be relocated to the GTE Chantilly, VA, facility. Remote diagnostic data communication from the Chantilly facility to the Boneyard would be via commercial telephone links and modems. A help-desk approach would be used first to resolve problems, then CORDS would be connected for computer-to-computer diagnosis if the help desk was unsuccessful. GTE personnel would collect the data. This evaluation was to be performed on a "not to interfere" basis with normal Boneyard activities.

4.2.1. Problems

- Although CORDS was eventually installed, delays pushed back the initial demonstration to April 1992. The system "crashed" at the beginning of the demonstration due to a thunderstorm-induced power surge. No evaluation data have been provided to SAIC at the time this report was published.

- Large equipment deliveries interrupted preparations for and performance of the evaluation on several occasions.

- As a result of, and in addition to, the interruptions caused by equipment deliveries, GTE personnel were diverted to higher priority tasking.

- The CATIS hardware that was available for CORDS testing was shipped for installation at another site before CORDS could be used. This not only impacted the evaluation of CORDS, but also the verification of faults in the pre-faulted modules.

- There were delays in developing the pre-faulted hardware modules due to the coordination required between the supplier and GTE and the time it took to identify and then produce the correct modules. GTE did not receive the modules until the beginning of April 1992. Once the modules were on hand, the faults were not verified until after the first week in August 1992 due to the unavailability of AN/GYQ-21(V) systems and because of higher priority tasking for the GTE technicians.

4.2.2. Lessons Learned

- The CORDS system is not yet mature enough to compete with Hercules capabilities.

- Developing and validating pre-faulted modules requires a long lead time and the application of a dedicated resource.

- The ad hoc evaluation methodology used for the Boneyard is not effective under tight project timeline constraints. The flexibility advantage initially envisioned turned out to have an even greater procrastination component. Even though there was ample time to perform this evaluation, the evaluation continued to be delayed for other priorities. Similar evaluations in the future should receive higher prioritization and should be subject to more formal planning and scheduling.

4.3. U.S. Army Foreign Science and Technology Center

The FSTC was selected as a site to allow evaluation of the CM/RD concept at an operational U. S. Army site with a large and diversified inventory. Hercules services would be provided to a CSP system and two special systems running on DEC hardware. Again, only unclassified error register diagnostic data would be transmitted to the Hercules center. This site is also unique in that the systems to be used in the evaluation were located in separate areas. Because of the location and physical separation, an individual evaluation was planned for each of the systems. The evaluations were scheduled to be accomplished sequentially, with the evaluations taking place over a period of three normal five-day work-weeks.

Draft site-specific scenarios and procedures for FSTC were completed and provided to HQ DA/DAMI and FSTC in January 1992. Updates to the draft procedures were coordinated and provided in March and again in April.

4.3.1. Findings

- FSTC personnel have been eager to participate in the CME. FSTC ADP management and information security personnel were actively involved in planning from the beginning of the project.

- On the basis of the site-specific scenarios, procedures, and checklist that SAIC provided, the U.S. Army developed and wrote ***Security Policy and Standard Operating Procedures for Remote Maintenance Diagnostics of Department of Defense Intelligence Information Systems.***

- It would have been possible to conduct the FSTC evaluation at the same time as the RL evaluation if additional pre-faulted modules could be obtained. However, DIA approval decisions drove the scheduling of the FSTC phase of the CME, thereby preventing any simultaneous evaluations.

- Data and information from the Hercules center indicate that the projected use of CM/RD for computer-to-computer data communications is infrequent enough that it is not cost-effective to use a dedicated circuit.

4.3.2. Problems

- On-site personnel and Hercules technicians found that National Secure Telephone System (NSTS) circuits were too noisy and unstable for data communications.

- There was difficulty in finding acceptable secure data communications. The initial plan for FSTC called for the use of two different devices and circuits -- STU-III as a back-up and NSTS as the primary circuit. However, as stated above, the NSTS links were unacceptable for data communications, and the STU-III devices became the planned primary means of communication.

- This evaluation was delayed for the same security coordination reasons as the RL evaluation. Although the site was relatively well prepared to conduct the evaluation, DIA would not approve FSTC participation until the results of the RL evaluation could be reviewed and approved.

4.3.3. Lessons Learned

- Good quality secure communication lines are required for computer-to-computer data transmission for CM/RD.

- CM/RD use of secure lines should be shared with other uses of the secure communications.

4.3.3.1. Joint Intelligence Center, Pacific

Initial plans identified the Naval Intelligence Command facility in Suitland, MD as a likely candidate for a CM/RD evaluation at a Navy site. In November 1991, JICPAC was identified as a more suitable facility. Although not an independent Navy site, it provided an opportunity to evaluate the centralized maintenance concepts under Navy implementations of national security policies, regulations, and procedures in a joint Services operational environment. CATIS and CSP systems were selected for use in the evaluation at JICPAC. Candidates being considered for communications include Defense Secure Network 3 (DSNET3), STU-III devices, and the NSTS. A primary means of secure communication was still being investigated when this report was published.

4.3.4. Findings

- JICPAC personnel have been enthusiastic about the CME. The site commander and the IDHS resource manager scheduled dedicated support for the CME. It was thought that the CME might assist with installation and integration problems as the site was being established. Unfortunately, the CME at JICPAC will not be conducted in time to help with those processes. However, the delay may provide some scheduling relief because site installation, integration, and accreditation activities essentially will be completed before any CME takes place at JICPAC.

4.3.5. Problems

- The CME at JICPAC was affected by the same communication and security policy and procedure coordination delays that affected the scheduling of the CME at the preceding sites.

- The CME project started without a Navy site being identified. Due to delays in other evaluations, this proved not to be a major factor, but it did result in additional coordination being required.

- JICPAC's distance from the Washington area and time zone differences made coordination and planning for the evaluation more difficult.

- A suitable secure communication circuit had not been identified or approved at the time this report was written.

4.3.6. Lessons Learned

- Long distance coordination involving the Services and multiple Agencies is a lengthy process. Communication among all participants is essential.

5.0 EVALUATION RESULTS AND IMPLEMENTATION RECOMMENDATIONS (CDRL H007)

5.1. Introduction

The ***Evaluation Results and Implementation Recommendations*** report, a stand-alone planning and coordination tool, was intended to be produced after site evaluation data were available. When delays to the evaluations made it clear that the evaluations would occur too late to meet original CDRL production schedules, the RDWG decided that enough information was available from the site surveys, coordination process, and previous feasibility studies to make useful implementation recommendations without full technical data.

5.2. Methodology

SAIC defined and reviewed the basic implementation processes and compared them to the earlier Remote Diagnostic Analysis project and the current CME project. This comparison showed that the CME is one of several steps to be taken on the path toward complete implementation of remote diagnostics and centralized maintenance for the IDHS community. SAIC's definition of the implementation processes is presented in the following paragraphs.

5.2.1. Basic Implementation Processes

The implementation process for centralized maintenance should follow the sequence of processes depicted in Figure 5-1. Implementation is already underway, as basic

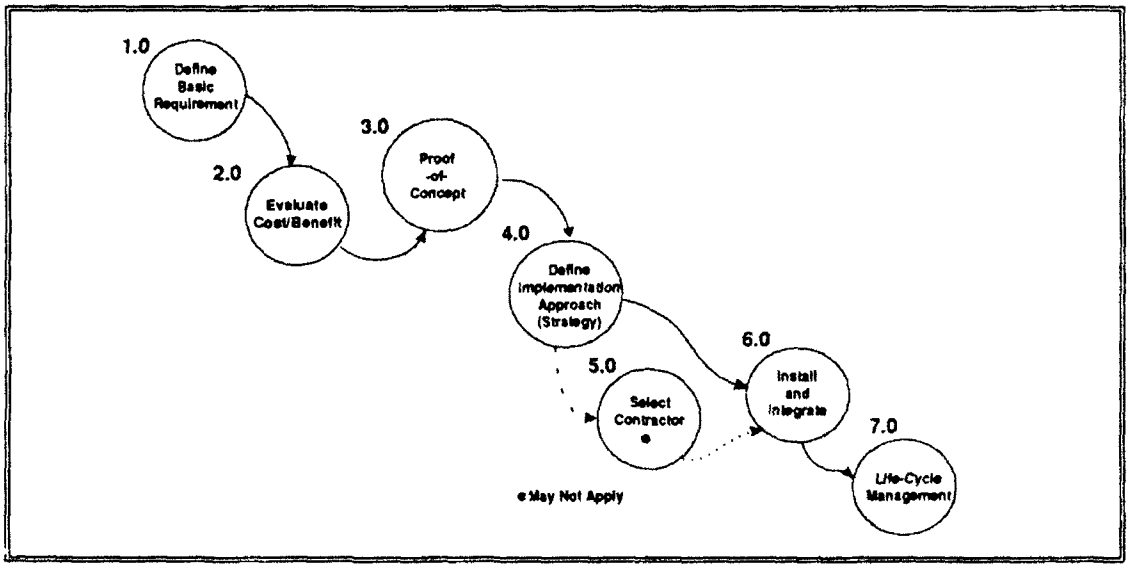


Figure 5-1 Basic Implementation Processes

requirement definition (Process 1.0) and cost/benefit evaluations (Process 2.0) were fundamentally accomplished during a preceding task and documented in the ***Remote Diagnostics Final Technical Report***. The CME task represents the proof-of-concept (Process 3.0) stage of the total implementation procedure. The next step in the implementation schedule is to select a specific approach and strategy for fielding remote diagnostics and centralized maintenance (Process 4.0).

5.2.1. Selecting and Planning the Approach

Figure 5-2 illustrates the activities associated with selecting and planning the most effective approach to centralized maintenance using remote diagnostics. Portions of

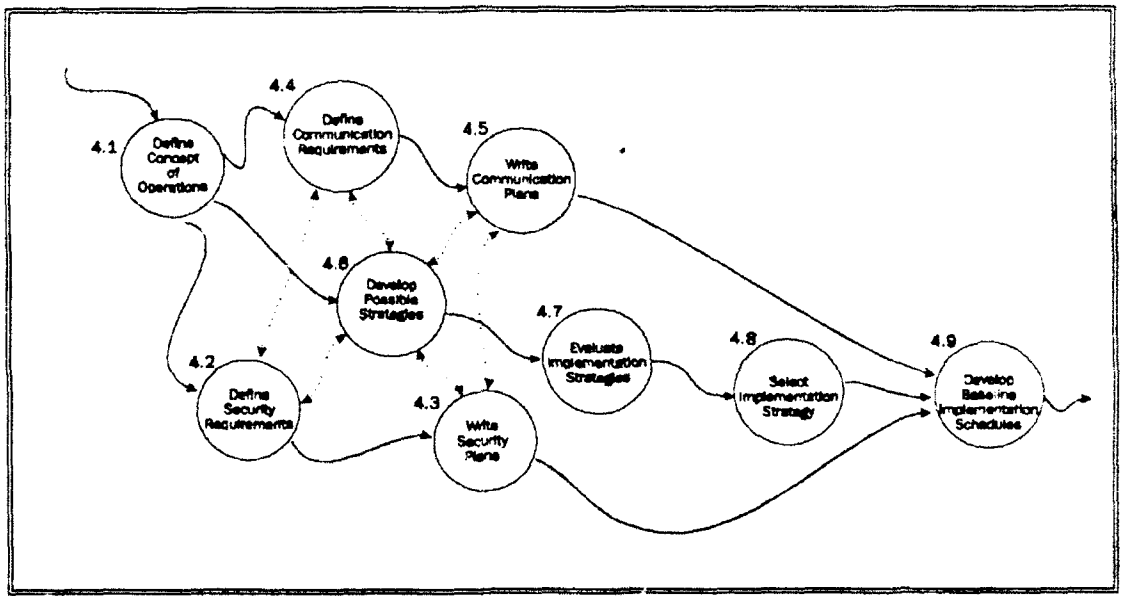


Figure 5-2 Implementation Strategy Definition Processes

this process have already begun under the CME effort, notably processes 4.1, 4.2, and 4.4, but more work is required to define and finalize the concepts of operations, security requirements and solutions, and communications requirements and solutions. There are many possible variables affecting the basic options. The definition of these variables and the options available from the variables are key elements of Process 4.6.

Figure 5-3 depicts the sub-processes of Process 4.6. Sub-process 4.6.1 was accomplished during the preparation of the implementation recommendations. Sub-process 4.6.2 was reflected in our analysis of the benefits and constraints associated

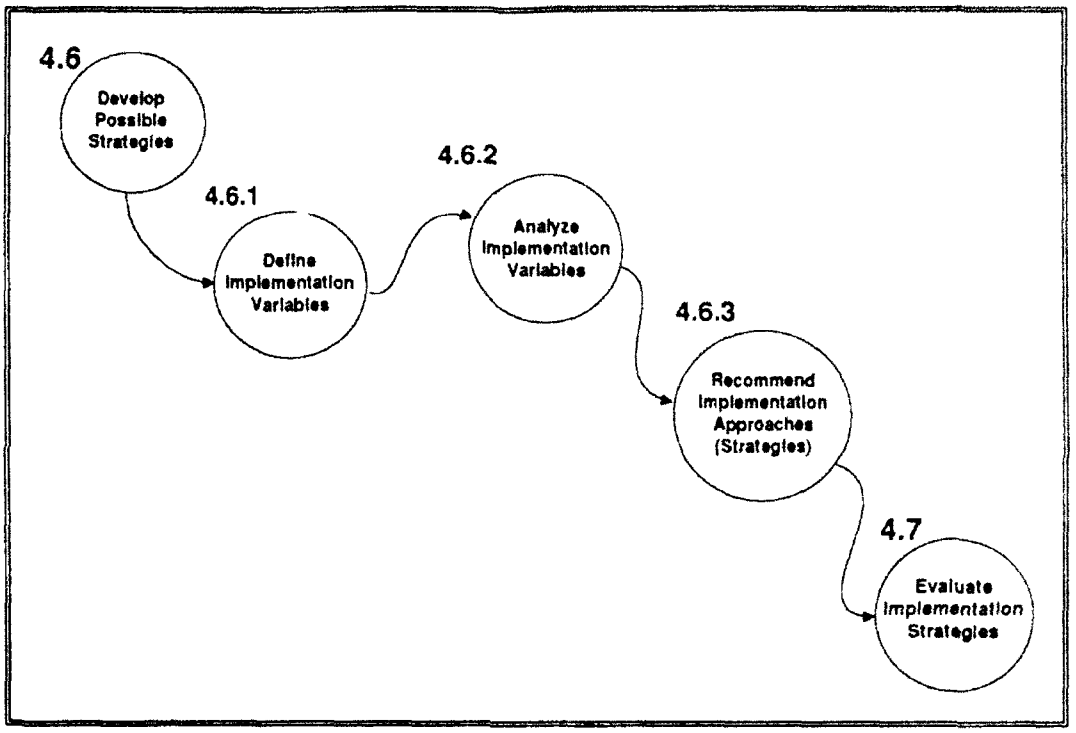


Figure 5-3 Process 4.6 - Develop Possible Strategies

with the implementation variables as described in the following paragraphs. This analysis was refined further with the addition of realistic assumptions facing the Government. We proposed our recommendations for implementation (Sub-process 4.6.3) to establish the foundation for Process 4.7.

The Government evaluated the recommended approaches (Process 4.7) and then selected their strategy (Process 4.8) based on these recommendations, the actual constraints, and the Government's own perceptions and priorities at the time of implementation.

5.2.2. Analysis

To analyze the options available to the Government and to propose an implementation approach based on the respective benefits and constraints of each option, SAIC first identified and described the variables that were factors in the implementation of CM/RD (Process 4.6.1). We grouped these by geographical distribution of services, ownership, and management responsibilities to include the options and associated prerequisites for success, which follow:

- Centralized Worldwide Diagnostic and Technical Support Center.
- Centralized Worldwide Logistics Services.
- Independent Regional Diagnostic and Technical Support Center.
- Independent Regional Logistics Services.
- Localized Diagnostic and Technical Support Center.
- Localized Regional Logistics Services.
- Hybrid Options for Diagnostic and Logistics Services.
- Government-Owned, Government-Operated Support System.
- Government-Owned, Contractor-Operated Support System.
- Contractor-Owned, Contractor-Operated Support System.

We then analyzed the constraints and benefits associated with implementing each of the above variables (Process 4.6.2), concentrating on the key driving issues of facilities, equipment, personnel, ease of management, operational reliability and responsiveness, time to implement, security, and associated costs. Tables summarizing these analyses are presented in Appendix E as Table 4, Table 5, and Table 6.

To provide a basis for meaningful recommendations, given the large range of variables, we imposed some realistic assumptions that were facing the Government. We then provided our conclusions identifying the most favorable characteristics for an implementation approach (Process 4.6.3), the Government requirements these would satisfy, and the remaining constraints and actions still required to implement such a scenario.

In concluding the analysis, SAIC evaluated the Government's current relative position with respect to such an implementation. Our conclusion was that use of the Hercules service at Ft. Meade, MD, offered the best existing candidate for near-term implementation; however, several total system requirements still remained to be satisfied.

5.3. Findings

- Enough information was available from the feasibility studies done prior to the CME project, from site evaluation coordination, and from Government experience with managing logistics to propose the basic options and recommended approach needed to take the next step in implementation planning.

- The security and communications constraints that hampered the site evaluation progress would apply under any scenario for implementation and appear to be solvable.

- The Government has many options available for implementation strategy. Although SAIC could choose a recommended path, the Government still had to do their own analysis of the variables and coordinate the choices that best satisfied all the individual priorities of the participants. This document also did not represent a black or white decision point. The implementation process will continue to evolve and details will be refined as choices are made between the variables.

- The Government cannot evaluate implementation of CM/RD without considering a multitude of options. A mix of diagnostic and technical support services and more traditional logistics services is required for the future. Therefore, cost/benefit tradeoffs between the variables of the two types of service will be necessary. As a result, a "whole system" approach to the full spectrum of logistics services is required for a long-term solution. This factor favors a hybrid approach to distribution of services, with some mix of centralized, regionalized, and localized support, to varying degrees for the combined set of services.

- It was possible to immediately eliminate the Contractor-Owned/Government-Operated support system as unrealistic from the start, concentrating instead on

Government-Owned/Government-Operated, Government-Owned/Contractor-Operated, and Contractor-Owned/Contractor-Operated options.

- There are few economies of scale from a facilities standpoint. A certain threshold (approximately 3500 square feet) is required as a minimum, yet Hercules has proven that such a facility can handle worldwide requirements without increases in space for added customers.

- The same is true for personnel, with a given staff able to handle significant increases in customer base without major expansions.

- Remote diagnostic system hardware and software requirements are also relatively independent of the number of customers and systems to be supported, although, there is likely to be some threshold for optimum performance.

- The less centralized the CM/RD approach, the more duplication is required for high cost items like facilities, equipment, and personnel to do a job that could be managed by a central facility/service.

- The main issue regarding ownership is whether the Government has suitable existing facilities or not. The construction or major modification of facilities is a high-cost, long-lead, and involved process.

- The biggest issues for operations are in the areas of personnel and training. Military manpower management is highly restrictive and relatively slow to respond to new requirements. The skills for remote diagnostic support are very specialized and are only developed with years of experience. The military system is not structured well for the low volume, high technology, long-term, intensive training and operations associated with remote diagnostics.

- Many Government constraints existed across all or most variables, or were relatively minor and subjective issues. This permitted the recommendations to focus on the significant variables of cost, facilities, manpower, and time to

implement. Several important assumptions could be made with some confidence regarding these areas, further focusing the conclusions.

- SAIC concluded that an implementation approach was favored with the following characteristics:

  - Use of a single, worldwide center concept, located in continental United States (CONUS).
  - Use of an existing, Government-owned facility, with established communications and security infrastructure in-place.
  - Use of an existing, or slightly modified set of equipment and documentation, either Government-Owned or Contractor-Owned.
  - Use of a Contractor-Operated, Contractor-supplied remote diagnostic and technical support service.
  - Continued use of some form of the current Contractor-Operated logistics service.

- SAIC found that the existing Hercules service satisfies sufficient requirements to proceed with immediate implementation actions. Although not technically under Government ownership, it is under tight Government control through the contract and performs its services from a Government facility with good communications possibilities to DoD user sites.

- A phased implementation would be most beneficial to the Government. Hercules can provide service to a large portion of the IDHS community. The existing regional and site-manned logistics structure is in place and functioning to offset Hercules deficiencies. The CM/RD concepts and technologies could mature to integrate CORDS-like capabilities into the whole system as they become available and are proven to operate in a secure environment.

5.4. Problems

- Site evaluations had not occurred, so detailed technical constraints and benefits could not be incorporated with assurances into the analysis.

- The absence of CORDS data effectively eliminated specific consideration of implementations involving this concept. A major portion of the "whole system" implementation approach had to be deferred by the Government until this, or similar, technology matures.

- In spite of the positive capabilities and features of Hercules, it still does not provide a total system solution to the implementation, as it is unable to service many networked workstations, some specialized AN/GYQ-21(V) peripherals, some deployable systems, and systems other than those which operate in a "system high" mode.

5.5. Lessons Learned

- Implementation of a complex, hybrid approach to CM/RD, worldwide and among multiple Service/Agency users, requires analysis of a very large set of variables.

- Given the above, some form of bounding and assumptions is necessary to focus implementation debate to a smaller set of realistic options before meaningful decisions can be made.

- Technical issues were not a major driver in the implementation approach analysis and decisions. Cost, resource management, facility availability, and practicality are the real issues. Much planning can be initiated on these factors alone.

- Careful analysis of the variables, especially of constraints and the responsibilities of the main participants, will lay much of the framework for specific implementation planning once an approach has been chosen.

- CM/RD has a minimum resource threshold, but with the capabilities of today's automation and communications technology, it is relatively independent of location, scale, or fluctuations in the using community.

- Technology and media exist to provide a successful implementation of CM/RD for AN/GYQ-21(V) systems. However, current ADP security policy will need to be

revised and procedures will need to be streamlined to implement this type of technical support in a timely and cost-effective manner.

6.0 IMPLEMENTATION PLAN (CDRL H008)

The Government accepted the course of action laid out by SAIC and, as a result, we produced a general implementation plan that described the activities involved in implementing CM/RD. SAIC first described the "whole system" approach as a series of four steps to achieve the complete solution.

1. Help-desk connection.

2. Computer-to-computer link for large systems.

3. Support for workstations and LAN servers.

4. Coordination between Hercules and Regional Support Centers.

We illustrated the implementation of CM/RD as a phased process, with phases overlapping and ongoing through the entire implementation period. Within these phases, we grouped the actions required to accomplish an effective operating CM/RD capability into several basic processes, some of which are already underway:

- Determine the implementation approach.

- Acquire or reallocate the necessary funding.

- Coordinate the details of implementation with users.

- Execute agreements to provide CM/RD services.

- Make adjustments to existing SSLSM operations.

- Resolve communications and security issues.

- Prepare the Hercules Center.

- Prepare the individual IDHS sites.

SAIC broke down these basic processes into sub-processes to provide a more detailed outline of the overall implementation plan. A diagrammatic presentation of these processes and sub-processes is included as Appendix F to this report.

6.1. Findings

- Due to existing logistics commitments, evolving security requirements, and varying maturity of CM/RD capabilities, a phased implementation will be the most practical. As a result, the Implementation Plan will require iterative updating as each phase is addressed in detail.

- The implementation of a help-desk capability can be accomplished relatively quickly, providing support for large numbers of sites at once.

- By first establishing the help desk, a significant level of support is provided and the communications and security constraints that impact the computer-to-computer phases are less a factor. Field engineers/technicians will also become familiar with using external assistance.

- Agreements and full coordination among all providers of logistics and maintenance services are required to achieve a full CM/RD implementation.

- The RDWG will continue to play a major role as advisors to the SSLSM Logistics Support Panel (LSP).

- Adjustments may need to be made to existing SSLSM contracts, task orders, CLINs, contractor manning and location, Government manpower positions, security billets, budgets, the Integrated Logistics Support Plan (ILSP), and/or user procedures.

- The full set of phased implementations will likely be satisfied through a combination of inter-agency agreements and additional and/or separate contract actions.

- The CME sites will be ready for accreditation and immediate implementation of full Hercules support if requirements and guidelines remain unchanged.

- The requirement for installation of secure voice systems is primarily a factor only at the Hercules center. Sites could relay problems through an intermediary secure voice location.

- An Installation and Integration (I&I) Team will be formed to plan and execute individual site surveys and installations.

- After the initial site implementations are successful, site-specific Installation and Integration Plans will become an iterative process. Coordination of communications connectivity, documentation, and schedules is critical.

6.2. Problems

- The CME is not yet complete. As a result, many of the detailed implementation processes and sub-processes will need to be modified. This is especially true for the unresolved security and communications issues. Accreditors have not approved a set of security guidelines, and specific technical solutions have not been determined.

- Implementation of the third step is largely to be determined. Although CORDS is being investigated to provide this service, the technology has not yet matured enough for implementation, and a provider of this service has not been established.

7.0 APPLICABILITY TO AN/GYQ-50(V) (CDRL H009)

SAIC and key members of the RDWG visited the IBM facility in Boulder, CO, where briefings concerning IBM's approach to remote hardware and software support were received. Information from the visit and findings concerning the applicability of CM/RD to AN/GYQ-50(V) was incorporated into user group briefings

7.1. Findings

- The concept of Centralized Maintenance Using Remote Diagnostics is applicable to AN/GYQ-50(V) systems. The IBM solution is currently applicable only to IBM systems and uses only IBM support and technical personnel. However, they do provide CM/RD services in a secure environment to classified Government customers.

7.2. Problems

- Implementation of CM/RD for AN/GYQ-50(V) will also encounter ADP security issues. IBM is currently attempting to demonstrate their system for the U.S. Special Operations Command at MacDill AFB, FL. However, the demonstration has been delayed until the ADP security issues can be resolved.

8.0 SUMMARY

In summary, the CME project was able to evaluate the CM/RD concept at one site — Rome Laboratory's Intelligence Information Processing Facility. In spite of this limitation, the Government was able to make significant progress toward planning for CM/RD implementation.

Detailed planning and time-consuming coordination among multiple Service, Agency, and contractor organizations were required to attain the authorizations and approvals for the demonstration and evaluation. The planning and coordination were hindered by the Defense Intelligence Agency's initial reluctance to participate in the planning. The CME was further impeded by a lack of DIA policy and procedures for a CM/RD concept. The development of pertinent policies and procedures was impacted by the reorganization activities at DIA and DISA as their new information system responsibilities and roles are being defined.

The Remote Diagnostics Working Group that was formed for this project provided an effective and efficient forum for coordination of multi-organization activities. However, effectiveness and efficiency would have been enhanced with active participation of the appropriate DIA decision-makers. As the implementation of CM/RD progresses toward actual fielding of CM/RD capabilities, more active participation will be required of DIA and DISA decision-makers.

The RDWG will continue to play an important role in the implementation of CM/RD capabilities. The implementation plan that was developed as a result of this project will serve as the basic plan for fielding and integrating CM/RD into the IDHS community. The plan will be modified to reflect maturing concepts and technology as CM/RD is fielded.

8.1. Lessons Learned

The major lessons learned from this effort were:

- The insufficiency of approved secure communications is a barrier to implementation of CM/RD, both from a technical and management perspective. There is a void in capabilities for low-volume, low-cost, approved secure-data communications between sites. Coordinating approval between at least three

different approval nodes (DIA, NSA, Site/Service representatives) is a time-consuming and lengthy process.

- CORDS is not yet mature enough to plan for effective implementation. Other vendors are pursuing similar CM/RD initiatives. Alternative CORDS-like capabilities may soon be available for assessment by the Government.

- Security approval authorities (e.g., DIA and NSA) are very unlikely to make rapid, decisive decisions in areas that fall between existing procedural guidelines.

- Responsible information security decision-makers and policy-makers must be involved in the planning and implementation of CM/RD.

- Current policy-making and policy-changing practices are unable to keep pace with rapidly changing technology and/or user demands for efficient solutions.

- A good working team, such as was found with the RDWG, can conduct planning rapidly and can review proposed plans and procedures quickly if these are developed and presented in an evolutionary manner.

APPENDIX A

Abbreviations and Acronyms

ADP	Automated Data Processing
AFISA/IND	Air Force Intelligence Support Agency, Directorate of Intelligence Systems
CATIS	Computer-Aided Tactical Information System
CDRL	Contract Data Requirement List
CM/RD	Centralized Maintenance using Remote Diagnostics
CME	Centralized Maintenance Evaluation
CONUS	Continental United States
CORDS	Central Operation Remote Diagnostic System
CSP	Communications Support Processor
DEC	Digital Equipment Corporation
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIIS	Department of Defense Intelligence Information System
DSNET	Defense Secure Network
FM	Funding Manager
FOC	Full Operational Capability
FSR	Field Service Representative
FSTC	Foreign Science and Technology Center
I&I	Installation and Integration
IDHS	Intelligence Data Handling System
IHPS	Intelligence Host Processing System
IIPF	Intelligence Information Processing Facility
ILSP	Integrated Logistics Support Plan
ISSO	Information Systems Security Officer
JICPAC	Joint Intelligence Center, Pacific
LSP	Logistics Support Panel
MILCON	Military Construction
NSA	National Security Agency
NSTS	National Secure Telephone System (Gray Phone)

O&M	Operations and Maintenance
OS	Operating System
PCO	Principal Contracting Officer
RDWG	Remote Diagnostics Working Group
RFP	Request for Proposal
RL	Rome Laboratory
SAIC	Science Applications International Corporation
SOW	Statement of Work
SSLSM	Single Service Logistics Support Manager
STU	Secure Telephone Unit
WR-ALC	Warner Robins Air Logistics Center

APPENDIX B
Relevant Documentation

The following documentation is relevant to centralized maintenance and remote diagnostics for AN/GYQ-21(V) systems. Included are documents from earlier related analyses and Government regulations.

Related Research

- ***Remote Diagnostics Analysis Interim Technical Report***, Science Applications International Corporation, 14 March 1991.
- ***Remote Diagnostics Cost/Benefit Analysis Interim Technical Report***, Science Applications International Corporation, 19 April 1991.
- ***Remote Diagnostics Final Technical Report***, Science Applications International Corporation, 12 June 1991.

Related Reports

- ***Remote Diagnostics Analysis Interim Technical Report***, Science Applications International Corporation, 14 March 1991.
- ***Remote Diagnostics Cost/Benefit Analysis Interim Technical Report***, Science Applications International Corporation, 19 April 1991.
- ***Remote Diagnostics Final Technical Report***, Science Applications International Corporation, 12 June 1991.
- ***Work Plan (Program Plan) for Evaluation of Centralized Maintenance***, Science Applications International Corporation, 16 September 1991.
- ***Technical Information Report, General Evaluation Plan for Centralized Maintenance Evaluation***, Science Applications International Corporation, 8 November 1991.
- ***Technical Information Report, Evaluation Results and Implementation Recommendations***, Science Applications International Corporation, 19 June 1992.
- ***Technical Information Report, Implementation Plan for Centralized Maintenance Using Remote Diagnostics***, Science Applications International Corporation, 30 July 1992.

Government Regulations

- Army Regulation 380-19, **Information Systems Regulation,** 1 August 1990.
- AF Regulation 205-1, **Information Security Program Regulation**, June 1986.
- AF Regulation 205-16, **Computer Security Policy**, 28 April 1989.
- AF Regulation 700-10, **Information Systems Security**, 15 March 1985.
- Executive Order 12356, **National Security Information**, April 6, 1982.
- Defense Intelligence Agency Manual (DIAM) 50-3, **Physical Security Standards for Sensitive Compartmented Information Facilities (U)**, February 1990.
- Defense Intelligence Agency Manual (DIAM) 50-4, **Security of Compartmented Operations, (C)**, June 24, 1980.
- Defense Intelligence Agency Manual (DIAM) 50-24, **Security Policy for Using Communications Equipment in a Sensitive Compartmented Information Facility (SCIF)**, August 31, 1990.
- Defense Intelligence Agency (DIA) **Security Handbook for Automated Information Systems (AISs) and Separately Accredited Networks and the Supporting Tutorial Documents**, DRAFT Version, January 1991.
- DoD Directive 5200.28, **Security Requirements for Automated Information Systems (AISs)**, March 21, 1988.
- DoD 5200.28-STD, **Trusted Computer System Evaluation Criteria**, dated December 1985, authorized by DoD Directive 5200.28, March 21,1988.
- DoD 5200.1-R, **Information Security Program Regulation**, June 1986.
- DoD Directive C-5200.5, **Communication Security (COMSEC) (U)**, October 6, 1981.
- DoD 5220.22-R, **Industrial Security Regulation**, December 1985.
- DoD 5220.22-M, **Industrial Security Manual for Safeguarding Classified Information**, January 1991.
- NACSIM 5203, **Guidelines for Facility Design and RED/BLACK Installation**, June 30, 1982.
- National Telecommunications and Information Systems Security Instruction No. 7000, **TEMPEST Countermeasures for Facilities (U)**, October 1988.
- MIL-HDBK-232A, **Military Standardization Handbook RED/BLACK, Engineering-Installation Guidelines (U)**, November 1972.
- SECNAVINST 5239.2, **Department of the Navy (DON) Automated Information Systems (AIS) Security Program**, 15 November 1989.

- SECNAVINST 5239.3, **Department of the Navy SCI/Intelligence Automated Information System (AIS) Security Program**, 23 July 1990.
- OPNAVINST 5239.1A, **Department of the Navy Automatic Data Processing Security Program**, 01 April 1985.
- USAFINTEL 201-1 (TS-CCO), **The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI) (U)**, 1 March 1986.

APPENDIX C

Remote Diagnostics Working Group

NAME	ORGANIZATION	PHONE
Carl Compton	AFISA/IND	(202)767-5396
Penny Johnson	AFISA/INDXS	(202)767-6048
Robert Chevier	RL/IRDW	(315)330-3629
Robert Herrman	RL/IRDW	(315)330-3126
Allen Burnell	HQDA, DAMI-AM	(703)697-1303
Barbara Gordon	HQDA, DAMI-AM	(703)697-1303
Larry Williams	NAVINTCOM	(301)763-3270
Irv Hite	NSA	(301)688-4386
Gary Fordham	WR-ALC/LKJL	(912)926-0880
Hilary Reeves	WR-ALC/LKJL	(912)926-0880
Earl Holthaus	DEC	(301)306-6626
Edward Merriel	DEC	(301)306-2753
Cal Benedict	GTE	(703)818-5300
James Barr	GTE	(703)818-5300
Dan Melendy	GTE	(703)941-1438
Robert Lambert	SAIC	(703)538-3700

APPENDIX D

Centralized Maintenance Evaluation Schedules

CDRL	TITLE	DUE	COMMENTS
H001	Monthly Status Report	Monthly	First Status Report due 8-Oct-91
H002	Cost Status Report	Monthly	Cost Status Reports will be delivered with each Monthly Status Report
H003	Program Plan (Work Plan)	16-Sep-91	Reflects Working Group inputs
H004	General Evaluation Plan (Draft)	25-Oct-91	Review by Working Group to provide Gov't Comments
H004	General Evaluation Plan (Final)	8-Nov-91	
H005	Evaluation Procedures		
	Rome Lab Site	(25-Nov-91)	Due date determined by actual site evaluation date
	"Boneyard" Site	(25-Nov-91)	Due date determined by actual site evaluation date
	Army Site	(6-Jan-92 - 13-Jan-92)	Due date determined by actual site evaluation date
	Navy Site	(1-Feb-92 - 14-Feb-92)	Due date determined by actual site evaluation date
H006	Evaluation Reports		
	Rome Lab Site	(27-Dec-91)	Due date determined by actual site evaluation date
	"Boneyard" Site	(27-Dec-91)	Due date determined by actual site evaluation date
	Army Site	(31-Jan-92 - 14 Feb-92)	Due date determined by actual site evaluation date
	Navy Site	(6-Mar-92 - 13-Mar-92)	Due date determined by actual site evaluation date
H007	Evaluation Report & Implementation Recommendations (Draft)	(6-Apr-92 - 13-Apr-92)	Gov't Comments at 17-Apr-92 Working Group Meeting
	Evaluation Report & Implementation Recommendations (Final)	(1-May-92)	Due date will be determined by date of completion of last site evaluation
H008	Implementation Plan (Draft)	(1-Jun-92)	30 Days after H007
	Implementation Plan (Final)	(3-Jul-92)	15 Days after draft comments received
H009	Presentation Materials	15-Nov-91	18-Nov-91 SSLSM Conference
		(20-Mar-92)	Pacific Conference
H010	Final Report (Draft)	(3-Aug-92)	
	Final Report (Final)	(30-Sep-92)	30 Days after receipt of Gov't comments

Table 1 Task 8 Schedule (Projected CDRL Delivery Dates)

(Extracted from ***Work Plan for Evaluation of Centralized Maintenance***, 16 September 1991.)

DATE	TYPE	PURPOSE	LOCATION
5-Sep-91	Initial Working Group	Contract kick-off & schedule development	Falls Church, VA
26-Sep-91	Expanded Working Group	General Evaluation Plan development	Falls Church, VA
25-Oct-91	Expanded Working Group	General Evaluation Plan Draft Review	Falls Church, VA
31-Oct-91	Working Group	Data Collection and In-progress Review	Boulder, CO (IBM)
21-Nov-91	Working Group	Review Rome & "Boneyard" scenarios	SSLSM Conference (WR-ALC)
5-Dec-91	Working Group	Pre-eval prep for Rome and "Boneyard"	TBD
19-Dec-91	Working Group	Initial review of Rome and "Boneyard" eval data	"Boneyard" (Alexandria, VA)
3-Jan-92	Working Group	Review final results of Rome and "Boneyard" data. Discuss procedures for Army and Navy site evaluations	Rome, NY
18-Mar-92	Working Group	Review all eval data. Implementation recommendation work-up. Review presentation materials for Pacific Conference	TBD
17-Apr-92	Working Group	Review and Gov't comment on Draft Evaluation Report and Implementation Recommendations	Falls Church, VA
4-May-92	Working Group	Initial Implementation Plan work-up	TBD
TBD-Jun-92	Working Group	Implementation Plan review	TBD
TBD-Jul-92	Working Group	Implementation Plan (Final) review	TBD
TBD-Aug-92	Working Group	As Required	TBD
TBD-Sep-92	Working Group	As Required	TBD

Table 2 Task 8 Projected Working Group Meeting Schedule

(Extracted from ***Work Plan for Evaluation of Centralized Maintenance***, 16 September 1991.)

CDRL	TITLE	DUE DATE**	COMMENTS	STATUS
H001	Monthly Status Report	Monthly	First Status Report due 8-Oct-91	Completed & Ongoing
H002	Cost Status Report	Monthly	Cost Status Reports will be delivered with each Monthly Status Reports	Completed & On-going
H003	Program Plan (Work Plan)	16-Sep-91	Reflects Working Group inputs	Delivered 16-Sep-91
H004	General Evaluation Plan (Draft)	25-Oct-91	Reviewed by Working Group to provide Gov't Comments	Delivered 24-Oct-91
H004	General Evaluation Plan (Final)	8-Nov-91	CM Evaluation schedule based on Gov't projections of evaluation dates	Delivered 7-Nov-91
H005	Evaluation Procedures			
	Rome Lab Site	(25-Nov-91)	Due date determined by actual site eval date (2 weeks before start of site eval)	Delivered 4 Feb 92, two weeks before projected site eval
	"Boneyard" Site	(25-Nov-91)	Due date determined by actual site eval date (2 weeks before start of site eval)	Delivered 25 Nov 91
	Army Site (FSTC)	(6-Jan-92 - 13-Jan-92)	Due date determined by actual site eval date (2 weeks before start of site eval)	Draft delivered - Final pending firm start-date
	Navy Site (JICPAC)	(1-Feb-92 - 14-Feb-92)	Due date determined by actual site eval date (2 weeks before start of site eval)	Draft delivered - Final pending firm start-date
H006	Evaluation Reports			
	Rome Lab Site	(27-Dec-91)	Due date determined by actual site evaluation date (Due 2 weeks after site eval end)	(Scheduled to start 14-Sep-92)
	"Boneyard" Site	(27-Dec-91)	Due date determined by actual site evaluation date (Due 2 weeks after site eval end)	CORDS Set-up, but eval on hold for higher priority tasks
	Army Site (FSTC)	(31-Jan-92 - 14 Feb-92)	Due date determined by actual site evaluation date (Due 2 weeks after site eval end)	Evaluation date pending results of Rome Lab eval
	Navy Site (JICPAC)	(6-Mar-92 - 13-Mar-92)	Due date determined by actual site evaluation date (Due 2 weeks after site eval end)	Evaluation date pending results of Rome Lab eval
H007	Evaluation Report & Implementation Recommendations (Draft)	(6-Apr-92 - to 13-Apr-92)	Originally scheduled for Gov't Comments at 17-Apr-92 Working Group Meeting, which was projected as 30 days after last eval finish date	Draft for Gov't review completed 4 June 92*
	Evaluation Report & Implementation Recommendations (Final)	(1-May-92)	Original due date was determined by projected date of completion of last site evaluation (Due approx. 60 days after last eval finish date)	Completed 19 June 92
H008	Implementation Plan (Draft)	(1-Jun-92)	Originally due 30 Days after H007	Draft for Gov't review completed 14 July 92*
	Implementation Plan (Final)	(3-Jul-92)	Originally due 15 Days after draft comments received	Completed 30 July 92
H009	Presentation Materials	15-Nov-91	18-Nov-91 SSLSM Conference	Completed
		(20-Mar-92)	Pacific Conference	Completed
H010	Final Report (Draft)	(3-Aug-92)	Slipped to accommodate eval date slips	1 September 92*
	Final Report (Final)	(30-Sep-92)	Originally due 30 Days after receipt of Gov't comments	30 September 92

Table 3 Revised Task 8 Schedule ** Original projections in parentheses * 7-day Gov't Review & Comment

APPENDIX E

Implementation Considerations

(Extracted from ***Evaluation Results and Implementation Recommendations***, 19 June 1992.)

Distribution Variables

	Definition	Benefits	Constraints
Worldwide	**Diagnostic/Technical Support:** • Single center at large location with direct comms to each site • Sufficient ADP & Manpower to support all sites **Logistics:** • Central storage facility & distribution system • On-call manpower • Control & manage spares inventory • Dispatch spares to regional depots	• Least expensive to implement • Only one set of hardware, software, documentation, & spares required to perform diagnostics • Fewest personnel required • Less training time • No dilution of performance • Easiest to manage • Location decisions may be irrelevant	• Large enough facility must be built/acquired/modified • Career management & training problems • No alternative locations in the event of a failure , threat action, or natural disaster • Risks loss of performance/ responsiveness due to resource overload • Less flexible to variances in user's performance requirements • Political implications in decision process • Less responsive in terms of logistics support
Regional	**Diagnostic/Technical Support** • Stand-alone centers serving a distinct region, i.e. Europe or the Pacific **Logistics:** • Stand-alone centers serving a distinct region, i.e. Europe or the Pacific • Probable management support from CONUS-based headquarters	• Provides alternative locations for military personnel rotations • Fewer sites demanding service at each center • Provides for backup centers • More responsive to users than worldwide center • May ease inter-service and/or regional politics	• Duplication of facilities, equipment, personnel, documentation, comms, and cryptologic resources • Increase probability of not finding suitable existing facilities • Additional security processing & accreditation • More complex management • Increased configuration management burden • Service may be inconsistent from center to center • Additional costs resulting from overseas locations
Localized	**Diagnostic/Technical Support:** • Small stand-alone centers in areas of IDHS concentrations, i.e. Hawaii or Washington, DC. • Local management & diagnostics system **Logistics:** • Local facility or small centers having sufficient FSRs, storage, and spares inventory on hand • Probable management from central headquarters	• Performance standards may be adjusted to suit local users • Most flexibility for manpower/career management • Least vulnerable to threat • More flexibility in providing backup/emergency service	• Higher probability of facility construction being required • More duplication of facilities, equipment, personnel, etc. • Most difficult to centrally manage • Extensive planning & coordination needed to reach FOC worldwide • Most security accreditation & investigations • Risks hardware & software configuration management problems • Lowest utilization of diagnostic & support systems • Greatest risk of inconsistent performance

Table 4 Distribution Variables

Ownership and Operation Variables

	Benefits	Constraints
Government Owned	• If facility exists needing little modification, facilities resource and management costs are minor • Easier accreditation and security management • Allows choice in the operation of the diagnostic and technical support service	• Generally must be located on Government installation • New construction & modifications require lengthy process to program, budget, & build • Requires assignment of additional base infrastructure personnel • Government must provide on-going O&M programming, budgeting, and accounting
Contractor Owned	• Contractor has full responsibility for operation of facilities and equipment • Government involvement reduced to contract negotiations, and management, financial and security oversight • Contractor has potentially wider range of site locations	• Choice of contractor may be based on location & timeliness of providing facility rather than quality of services • Greater burden on ensuring that facility meets security requirements • Contractor rates increase over time and are difficult to budget for
Government Operated	• Gives Government greatest control over the service system • May be easier to acquire funding • Contracting process is avoided	• Facilities and equipment must be Government-owned • Most manpower intensive for the Government • Need to establish specialized training program • Possible problems in coordination between Services/Agencies • Career paths limited for military personnel • May result in lower quality technicians than contractor operated • Greater management burden to the Government
Contractor Operated	• Government manpower requirements are at a minimum • Reduced management burden for the Government • Less training required • Costs managed under single accounting system • Higher, more constant level of performance under contractual agreements • Consistent service across all sites	• Government must provide contractual oversight • Government may have less control over the exact desired services • Arrangements must be made to allow contractor access to Government sites • Government must conduct clearance and access investigations on civilians • Government must account for provision of services during periods of conflict

Table 5 Ownership and Operation Variables

PREREQUISITES FOR FUNCTIONING SYSTEMS

	GO/GO	GO/CO	CO/CO
Government:			
Occupy, construct, or modify a suitable facility(s) for diagnostic and technical support service at each site having a center	●	●	
Occupy, construct, or modify a suitable facility(s) for logistics and maintenance support services at each site having a center	●	●	
Budget MILCON and facility O&M funds as appropriate	●	●	
Program & budget O&M funds for contractor support		●	●
Separately program, acquire, test, and install necessary hardware equipment and software to perform services	●	●	
Program & budget manpower positions for each specialty required	●		
Program & budget manpower positions for facilities & base support personnel	●	●	
Acquire security billets and process investigations for Government personnel as required	●	●	
Acquire security billets for contractor personnel		●	●
Provide facilities' security (Military Police, access control, etc.)	●	●	
Assign and train all necessary personnel to initiate operations	●		
Assign, train, and manage manpower positions for any additional facilities support personnel required	●	●	
Ensure a manpower management system for training and rotating personnel on a regular basis as part of force management	●		
Establish a Government management structure	●		
Accredit the facilities, communications, and equipment as secure	●	●	●
Establish communications and cryptologic accounts	●	●	●
Establish acceptable contract vehicles		●	●
Contract for the services and periodically recompete the contract		●	●
Provide management and contractual oversight for performance of services and financial matters		●	●
Provide for support to deployed systems (exercise or crisis)	●	●	
Contractor:			
Hire and train a support cadre of managers, engineers, & administrators		●	●
Initiate and process security investigation paperwork on staff requiring clearances and accesses		●	●
Provide a minimum level of facilities for management and administrative staff		●	
Lease, purchase, or build facility(s) for equipment and personnel			●
Modify facilities to achieve required security levels			●
Acquire, test, and install required hardware and software		*	●
Operate the system		*	●
Provide in-house maintenance of equipment and operate facility		*	●

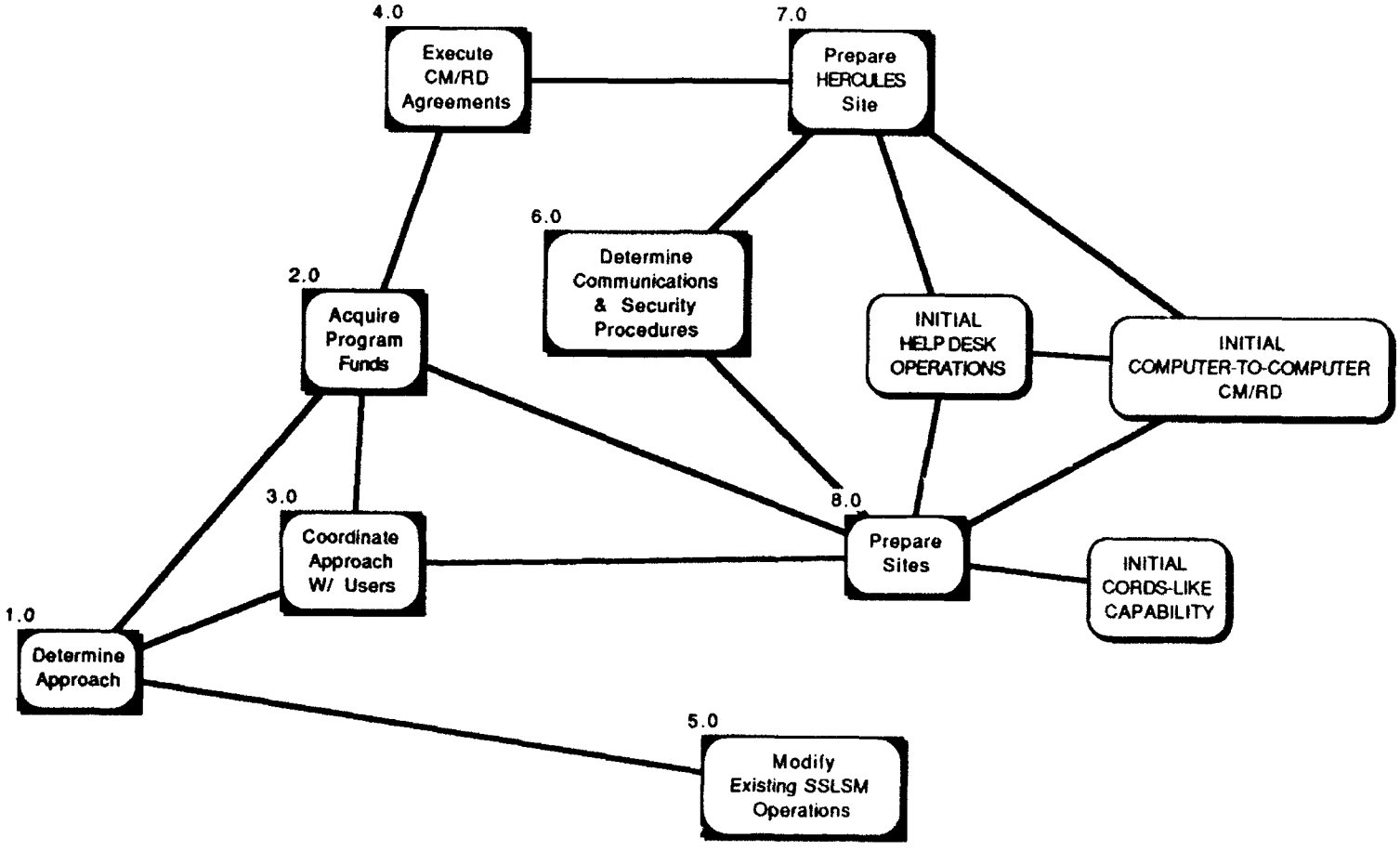
* May be a shared responsibility

Table 6 Prerequisites for Functioning Systems

APPENDIX F

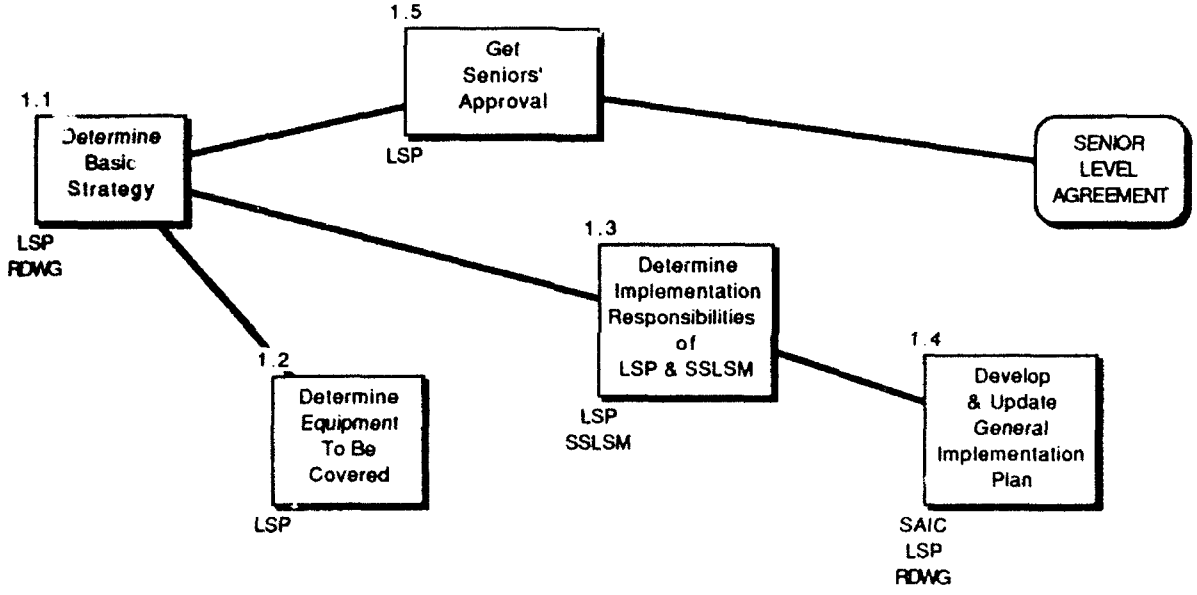
CM/RD Implementation Plan Diagrams

(Extracted from ***Implementation Plan for Centralized Maintenance Using Remote Diagnostics***, 30 July 1992.)



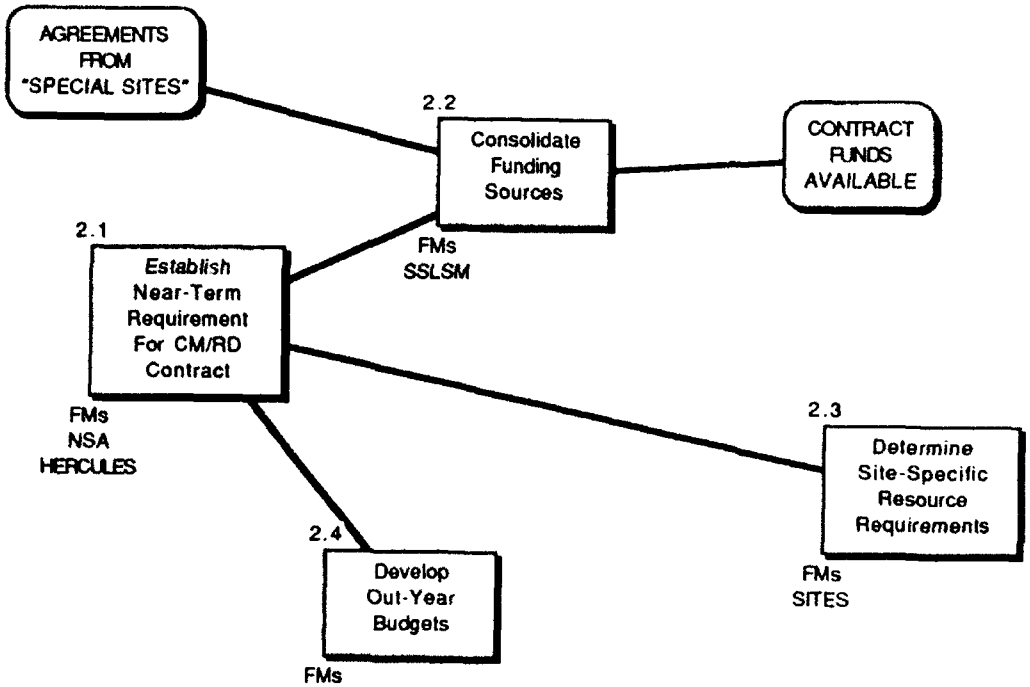
CM/RD IMPLEMENTATION PLAN
(LEVEL 0)

Figure F-1



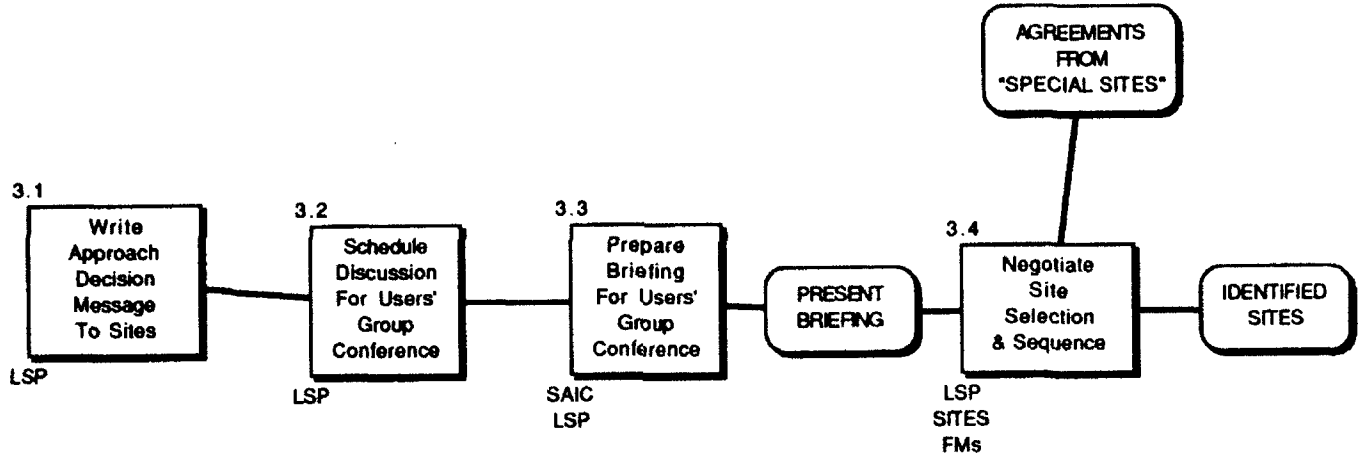
DETERMINE APPROACH (1.0)

Figure F-2



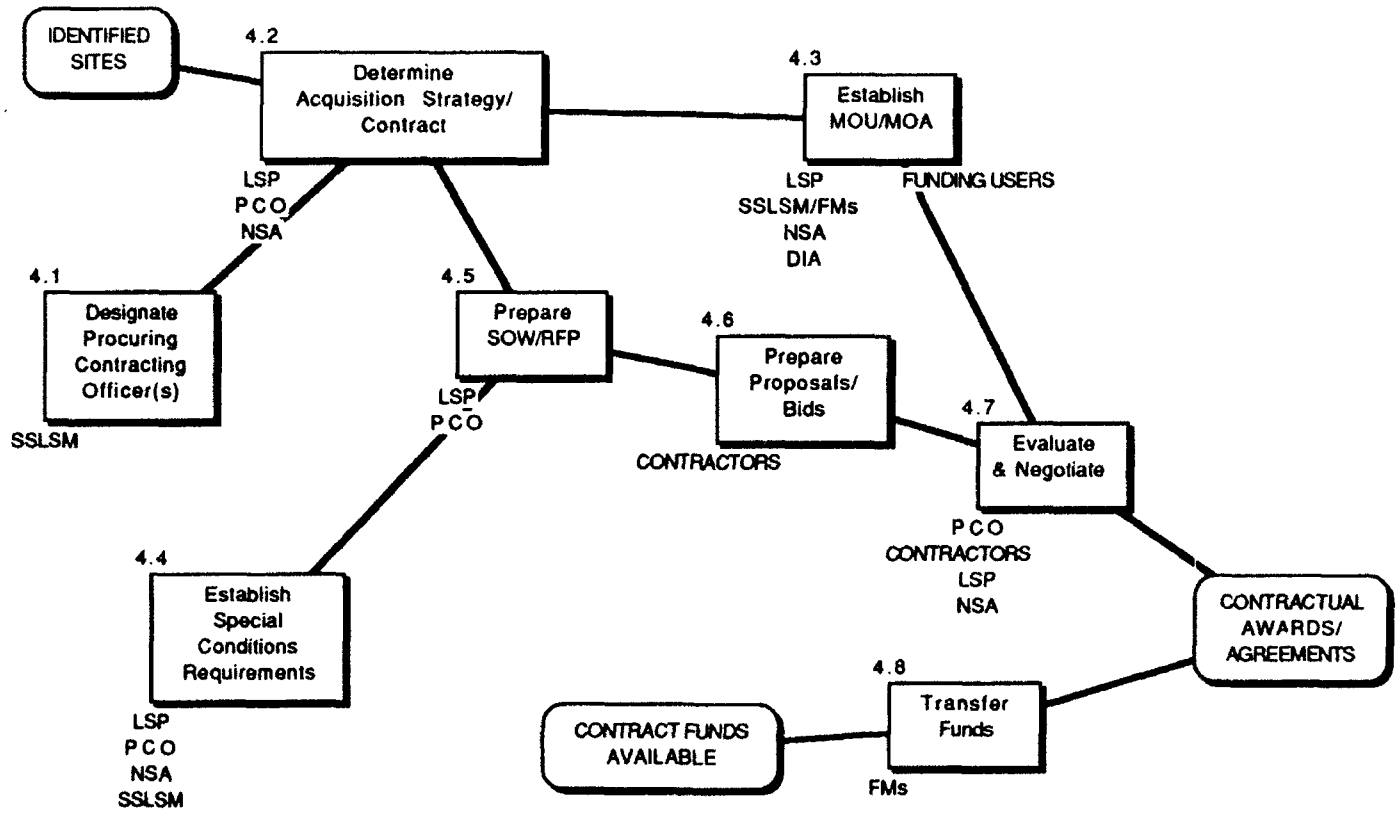
ACQUIRE PROGRAM FUNDS (2.0)

Figure F-3



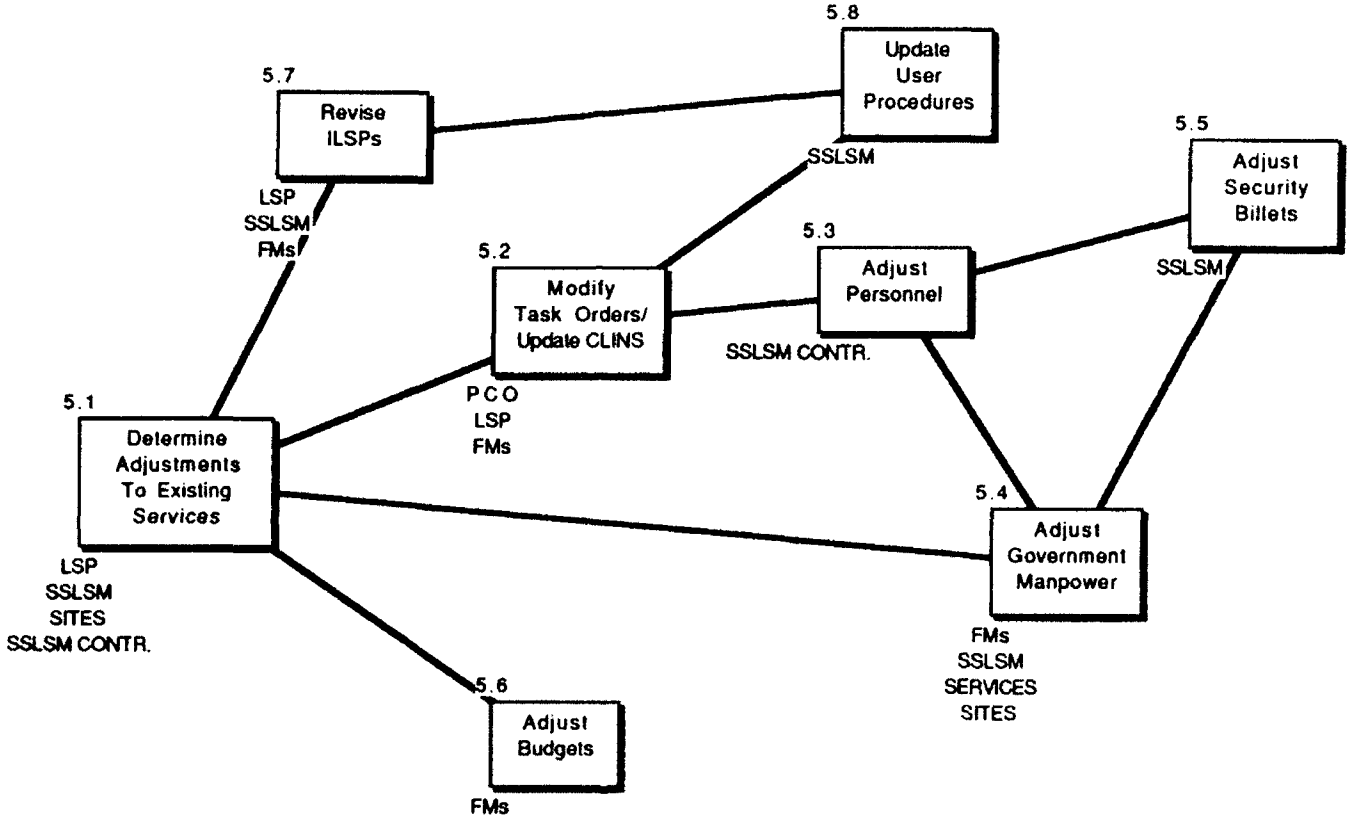
COORDINATE APPROACH WITH USERS (3.0)

Figure F-4



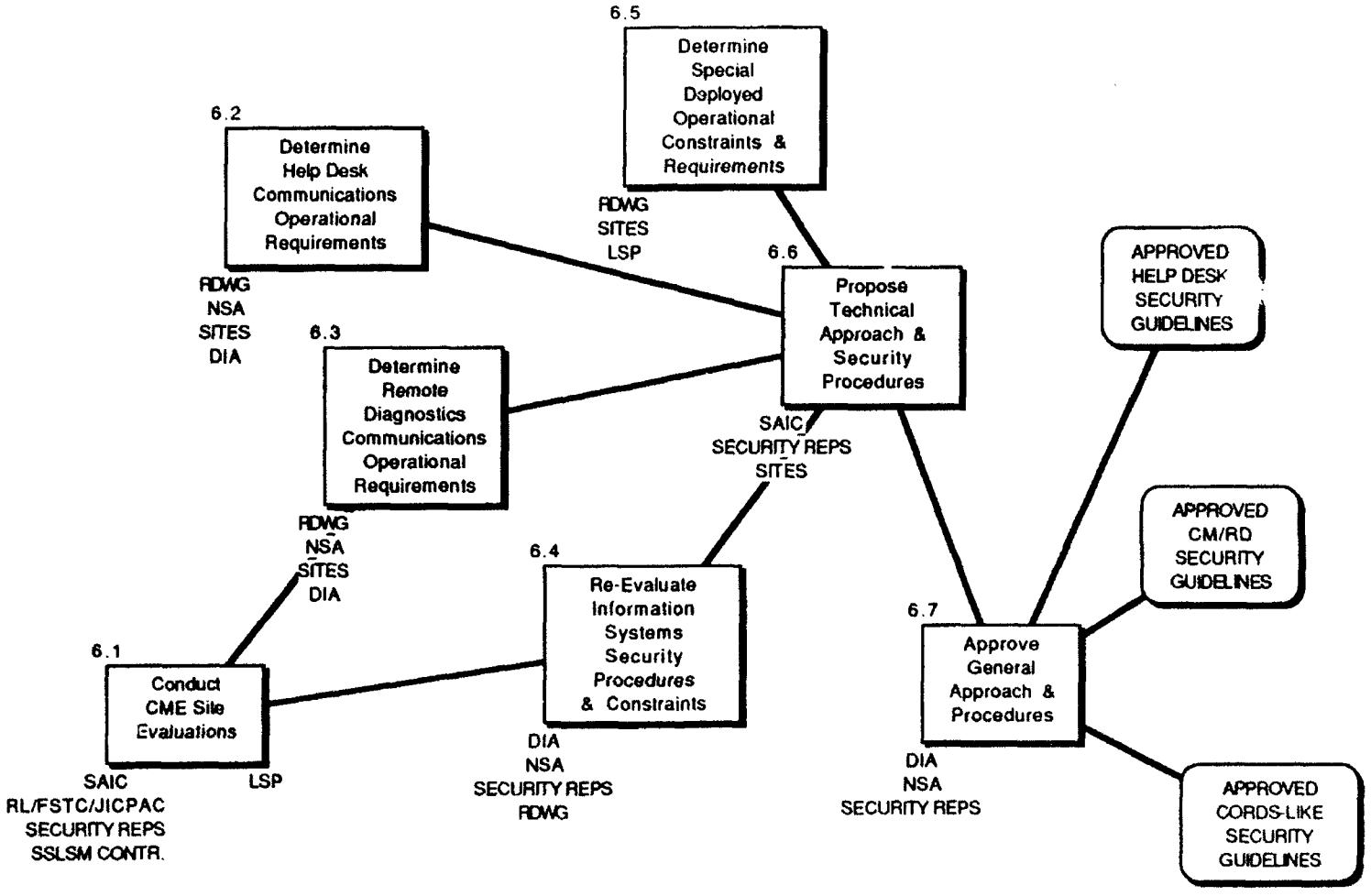
EXECUTE CM/RD AGREEMENTS (4.0)

Figure F-5



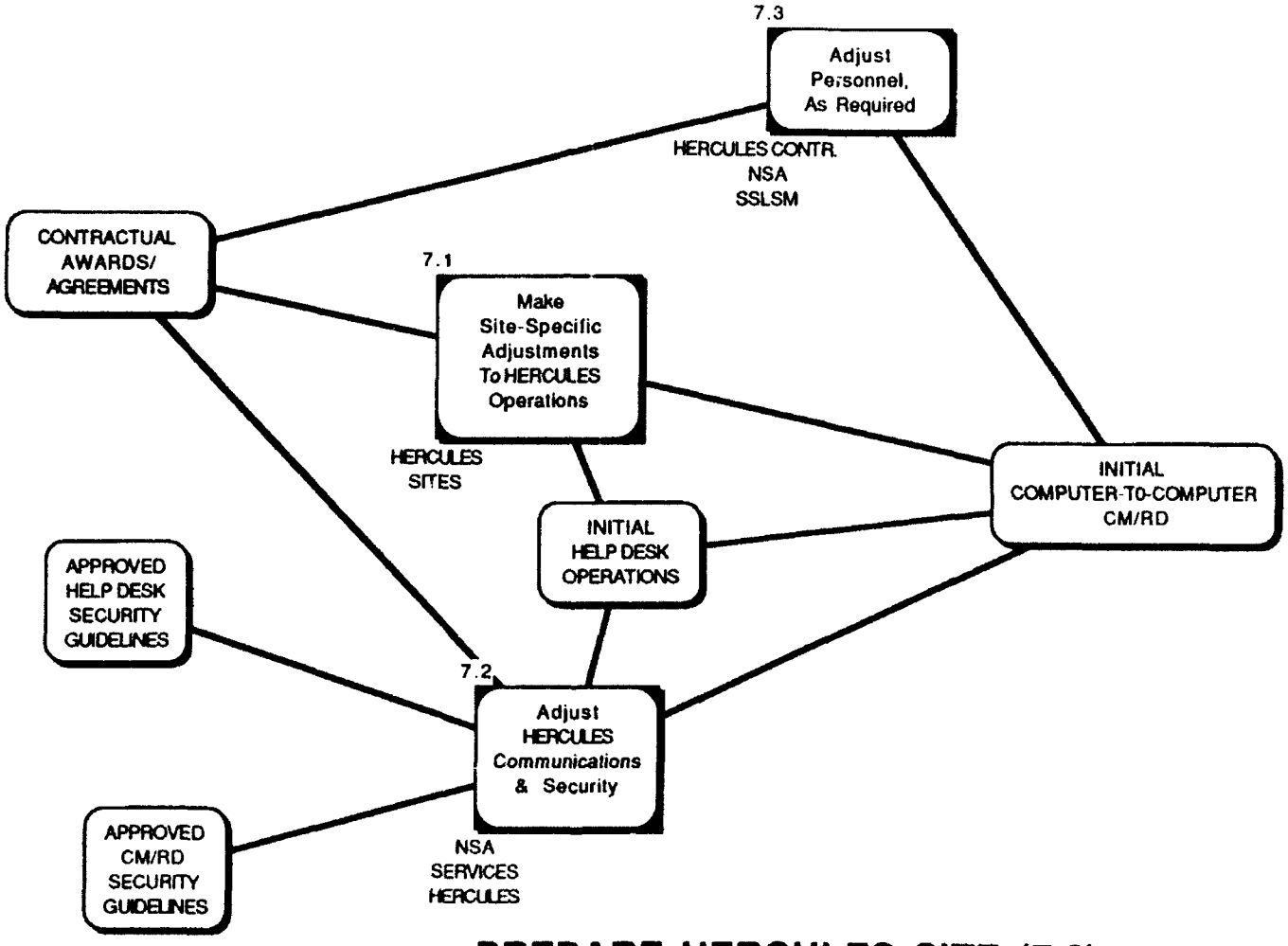
MODIFY EXISTING SSLSM OPERATIONS (5.0)

Figure F-6



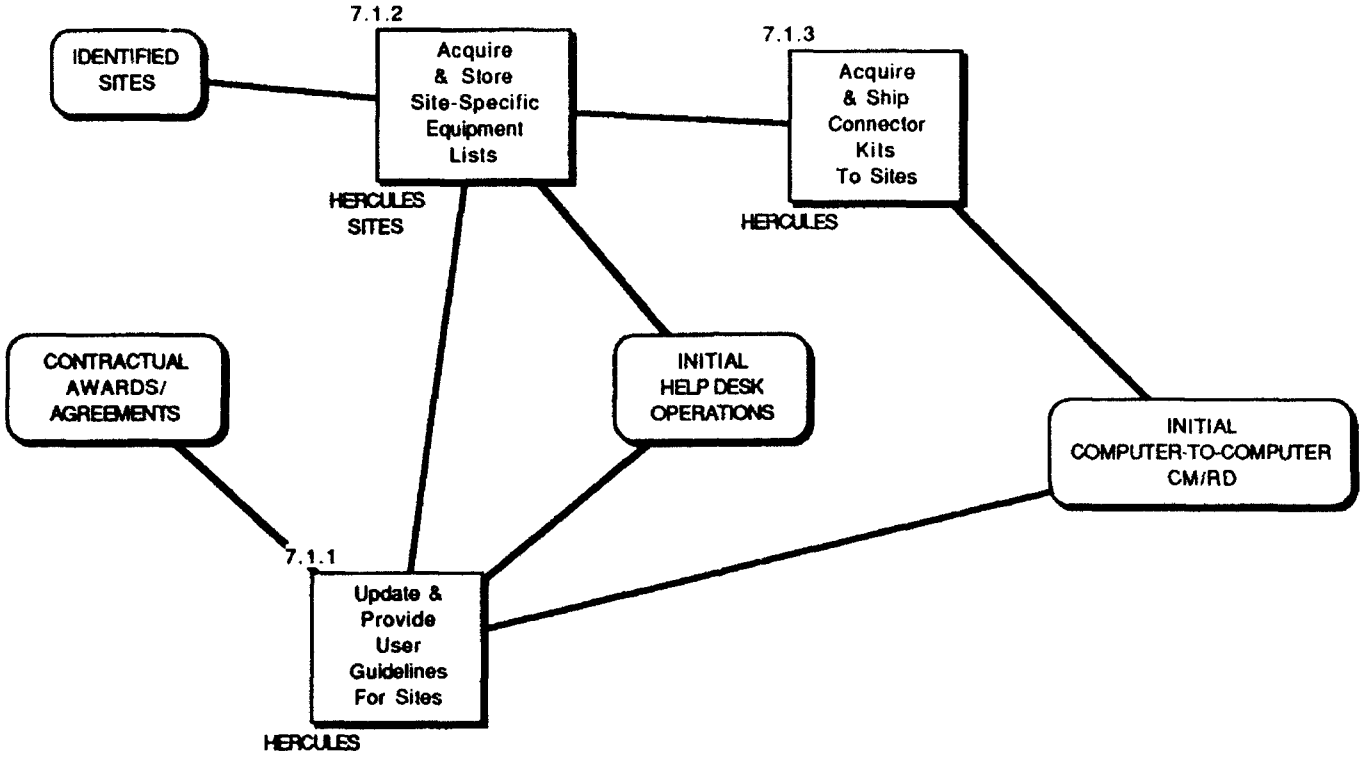
DETERMINE COMMUNICATIONS AND SECURITY PROCEDURES (6.0)

Figure F-7



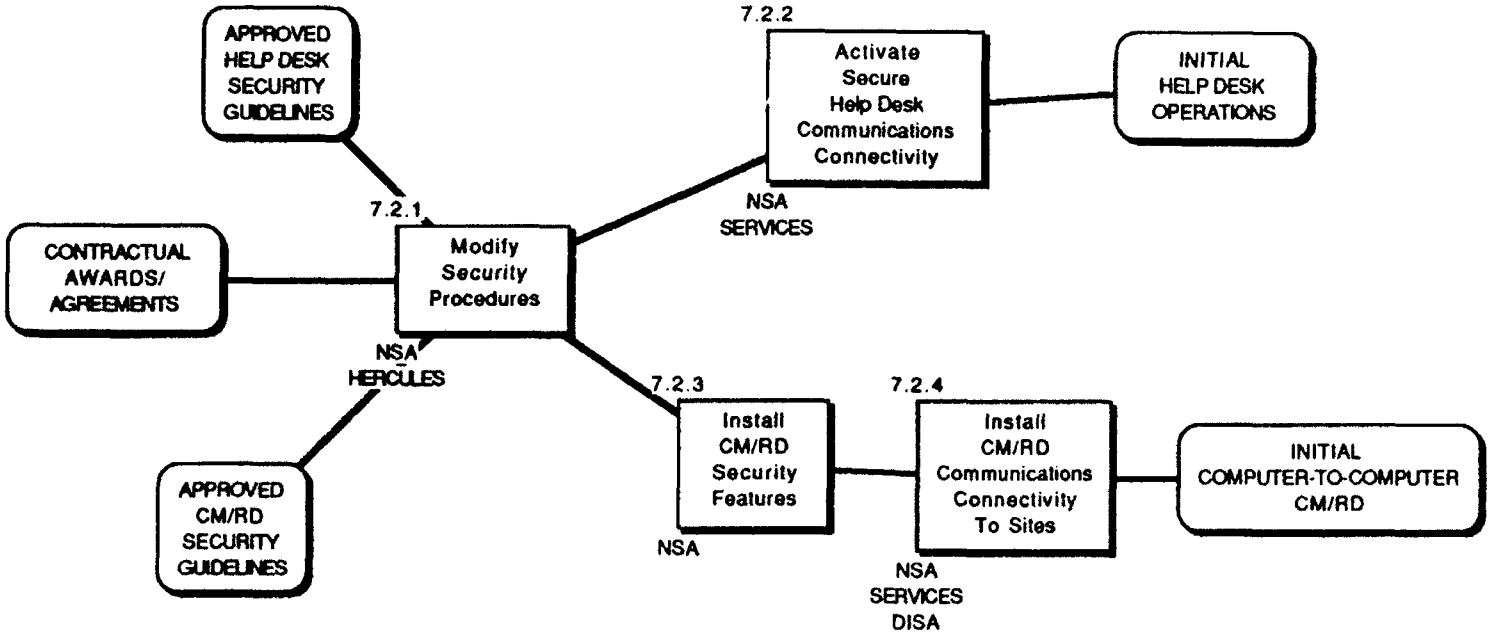
PREPARE HERCULES SITE (7.0)

Figure F-8



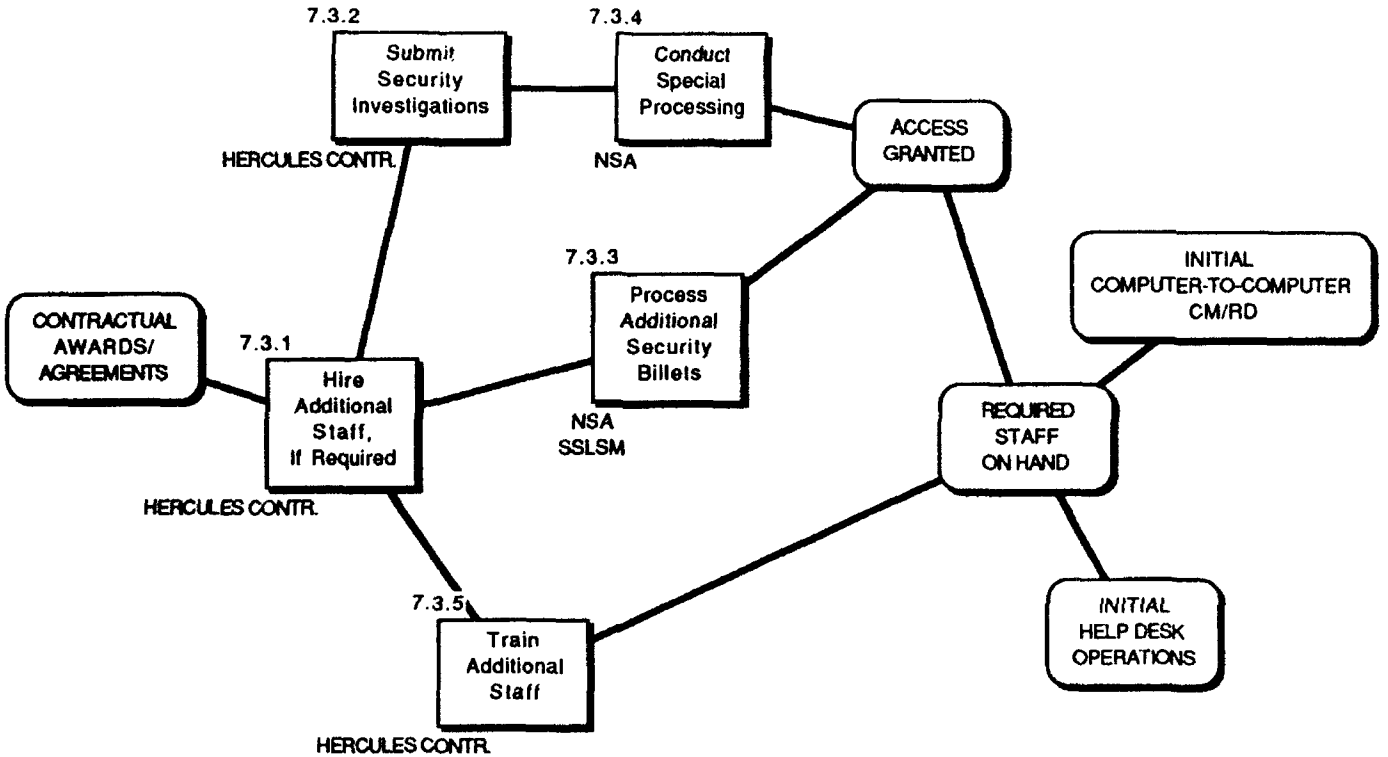
MAKE SITE-SPECIFIC ADJUSTMENTS TO HERCULES OPERATIONS (7.1)

Figure F-9



ADJUST HERCULES COMMUNICATIONS & SECURITY (7.2)

Figure F-10



ADJUST HERCULES PERSONNEL, AS REQUIRED (7.3)

Figure F-11

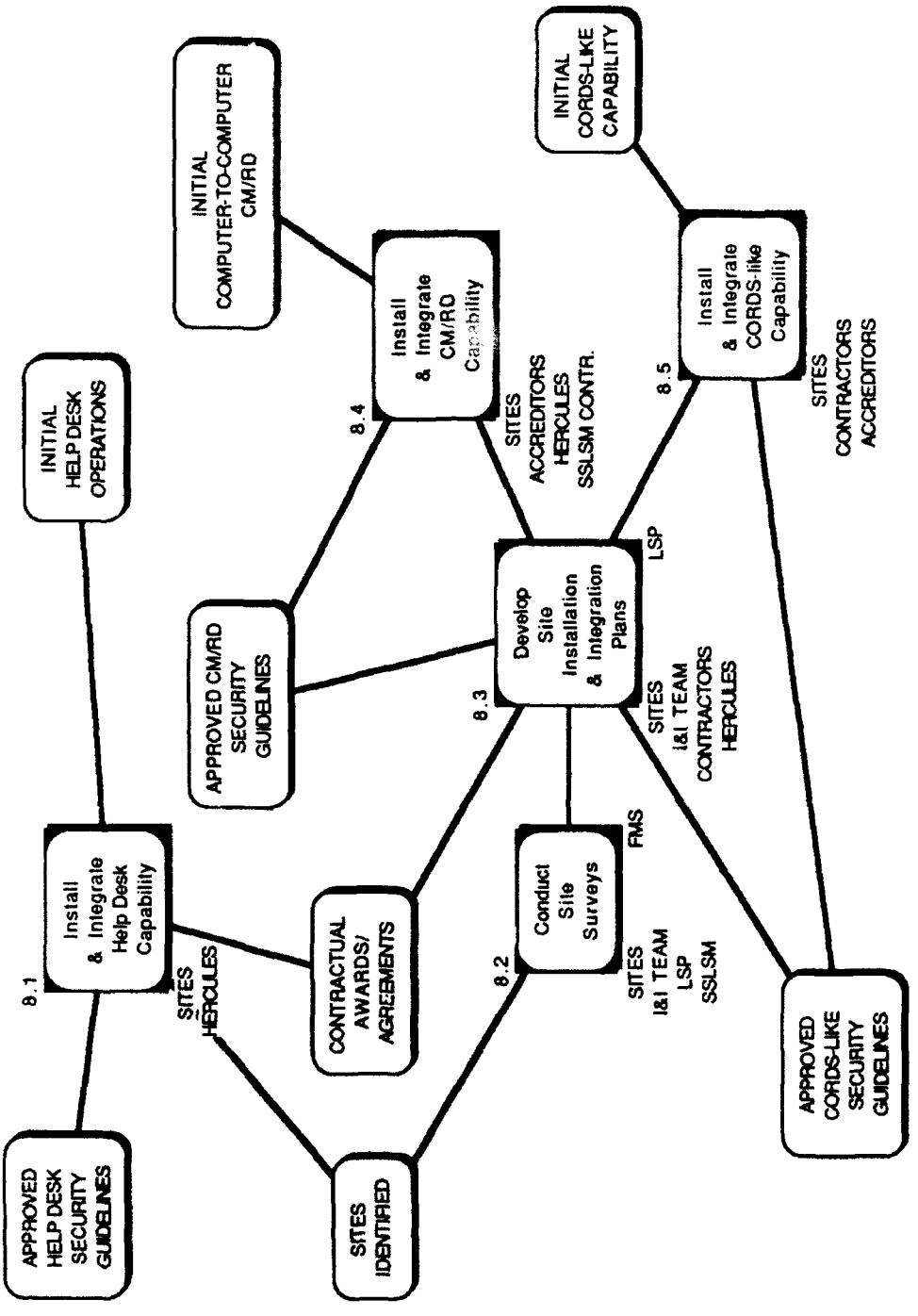
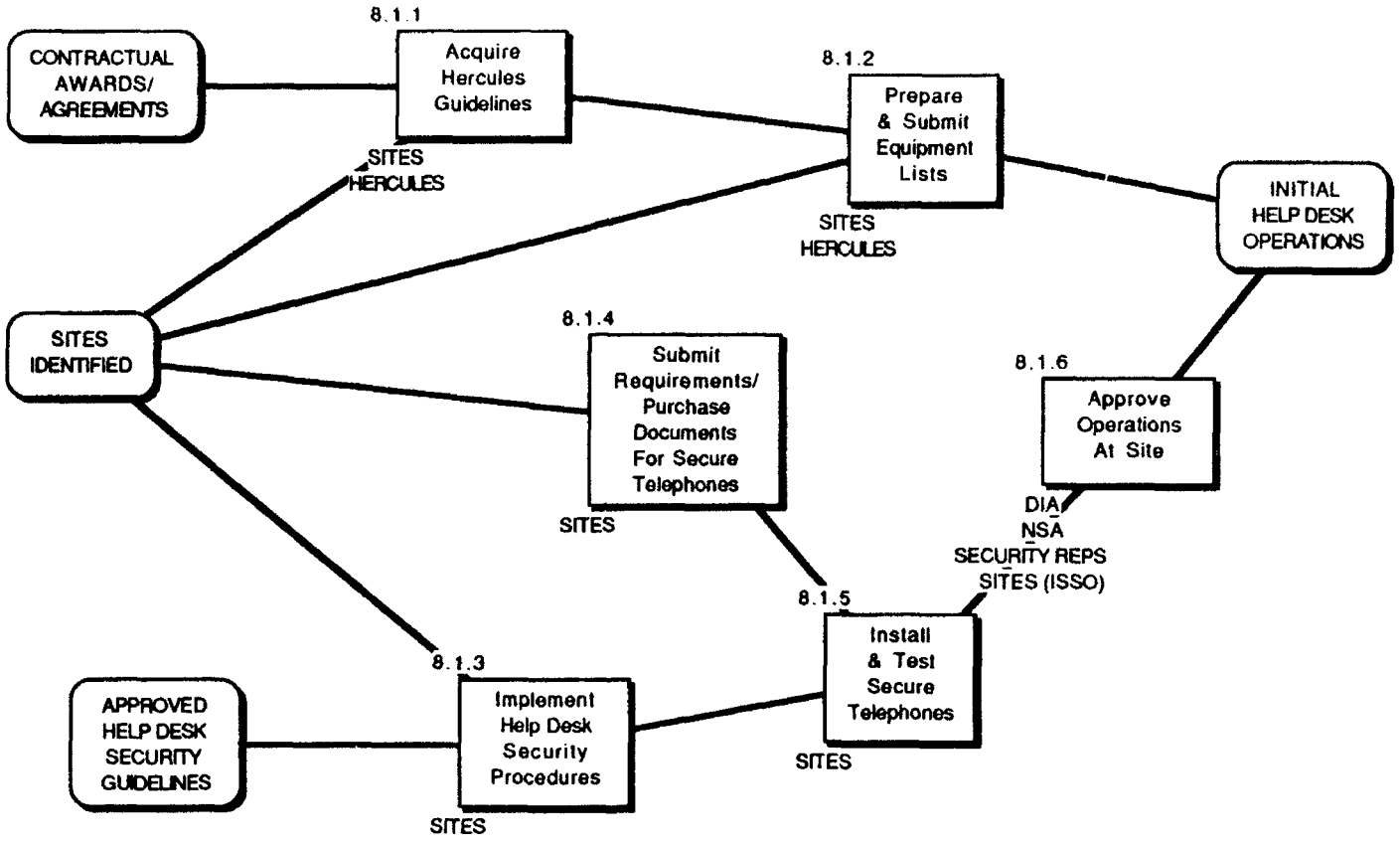
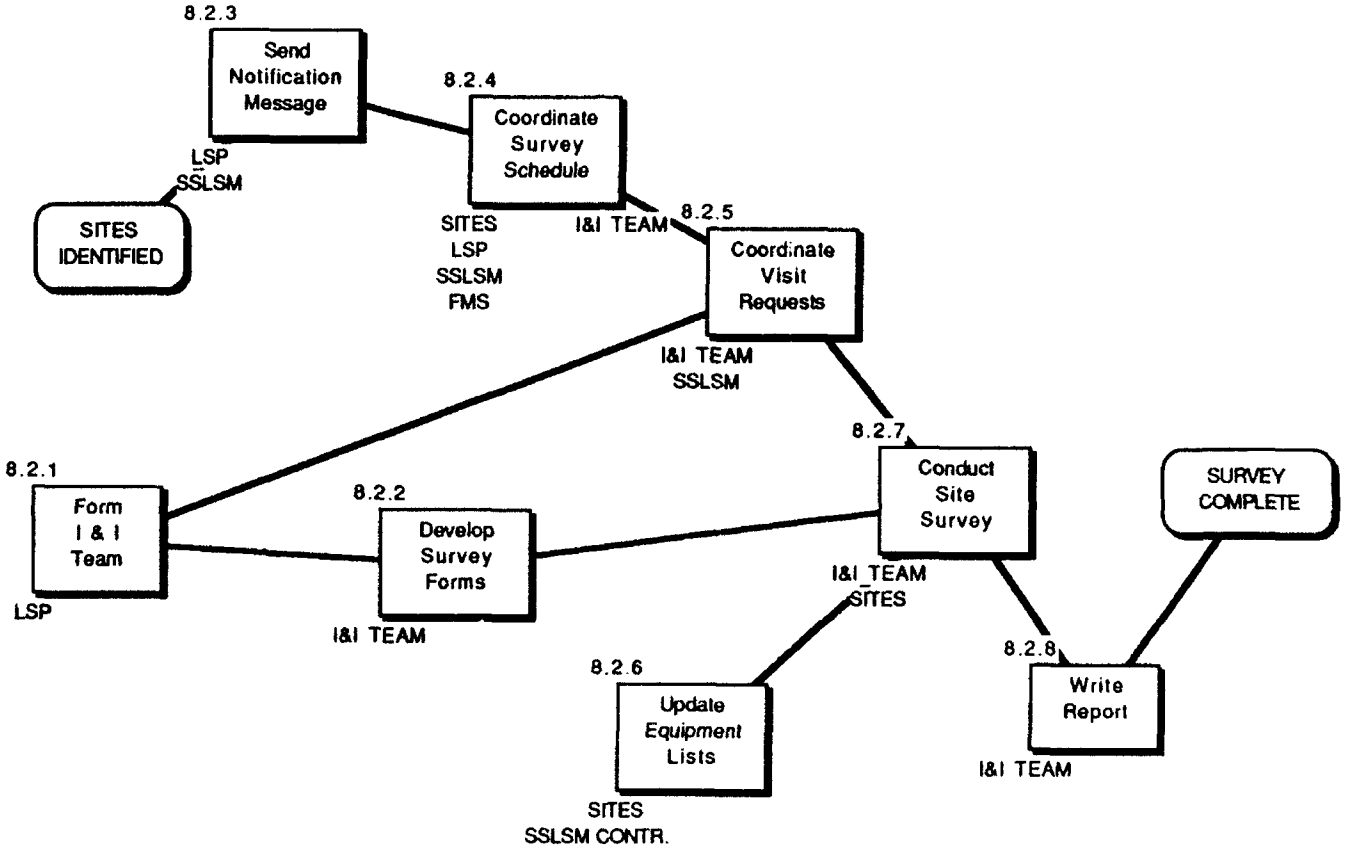

PREPARE SITES (8.0)
INITIAL COMPUTER-TO-COMPUTER CM/RD
INITIAL CORDS-LIKE CAPABILITY
INITIAL HELP DESK OPERATIONS
Install & Integrate CM/RD Capability
Install & Integrate CORDS-like Capability
8.4
8.5
SITES ACCREDITORS HERCULES SSLSM CONTR.
SITES CONTRACTORS ACCREDITORS
APPROVED CM/RD SECURITY GUIDELINES
Develop Site Installation & Integration Plans
LSP
8.3
SITES I&I TEAM CONTRACTORS HERCULES
Install & Integrate Help Desk Capability
Conduct Site Surveys
FMS
8.1
8.2
SITES HERCULES
CONTRACTUAL AWARDS/ AGREEMENTS
SITES I&I TEAM LSP SSLSM
APPROVED HELP DESK SECURITY GUIDELINES
SITES IDENTIFIED
APPROVED CORDS-LIKE SECURITY GUIDELINES

Figure F-12



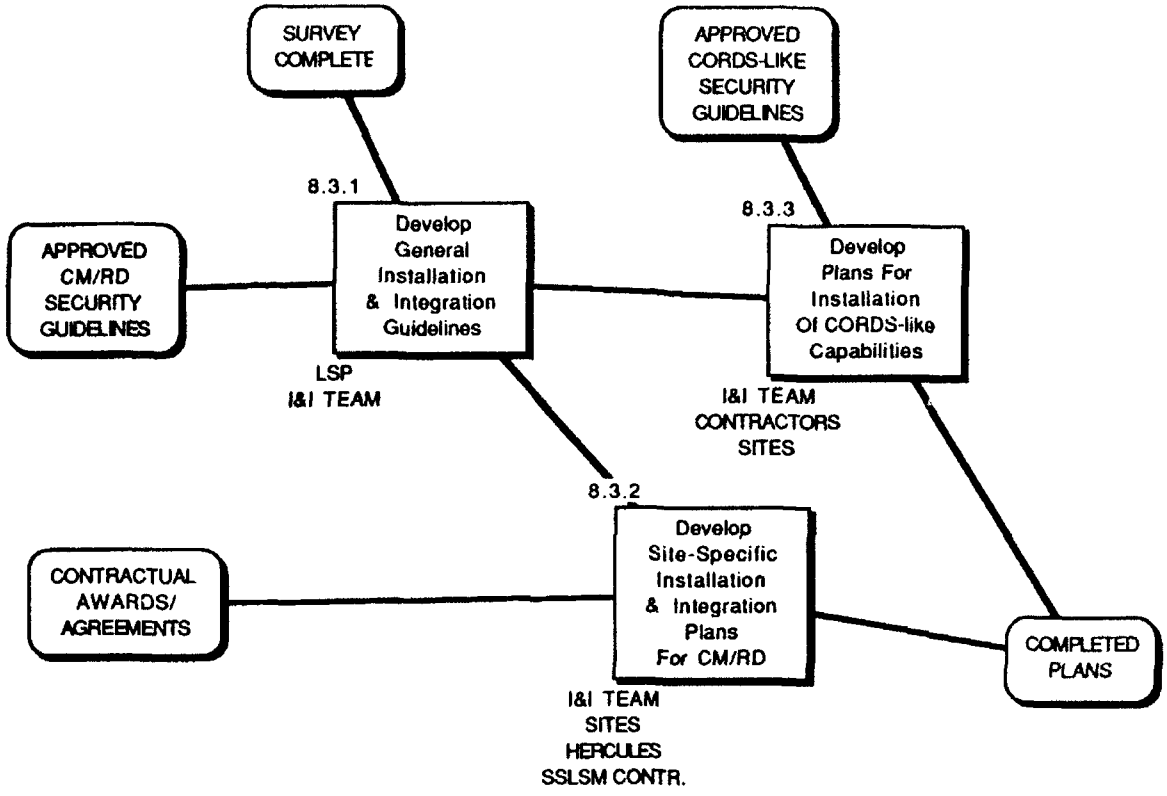
INSTALL AND INTEGRATE SITE HELP DESK CAPABILITY (8.1)

Figure F-13



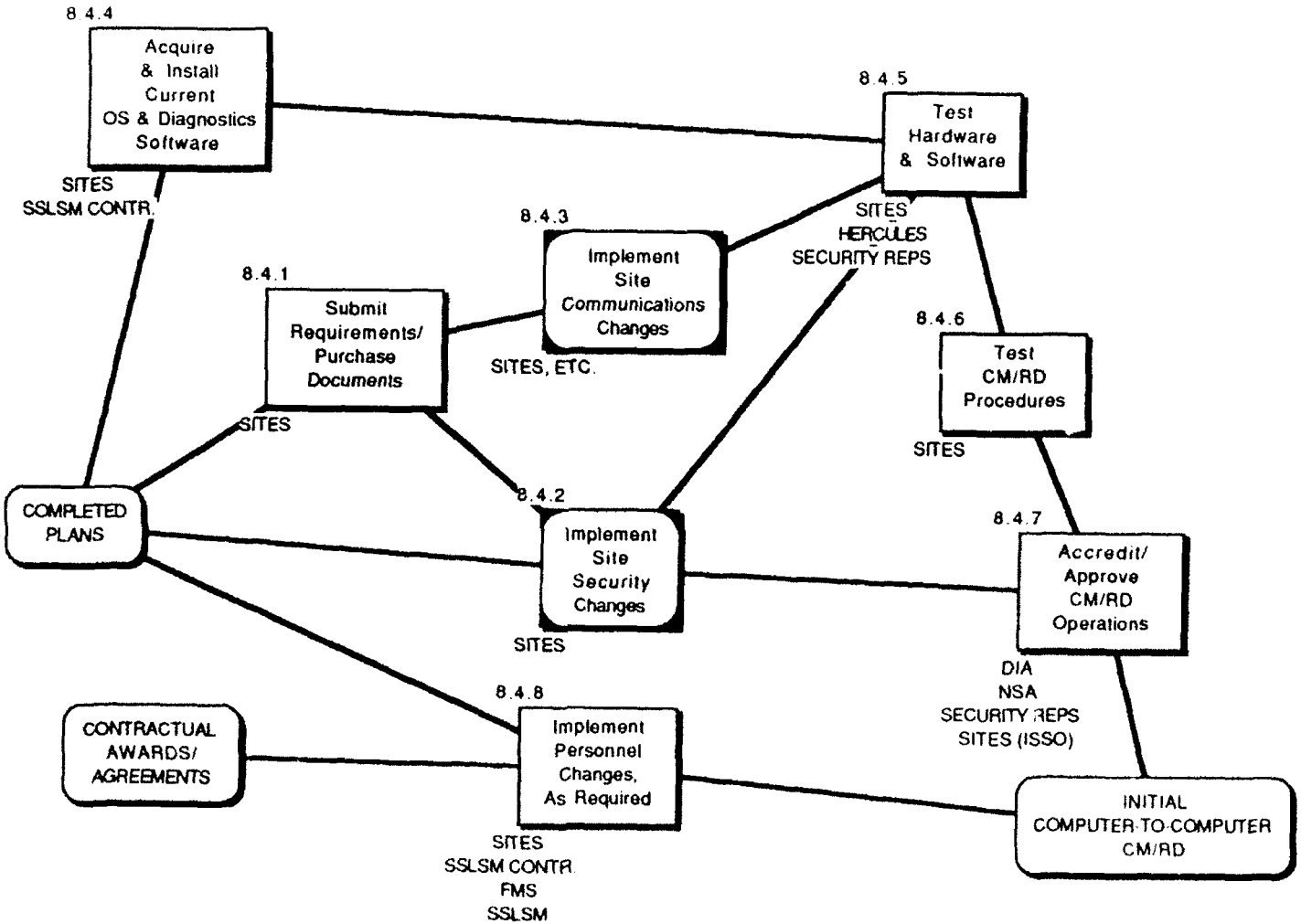
CONDUCT SITE SURVEYS (8.2)

Figure F-14



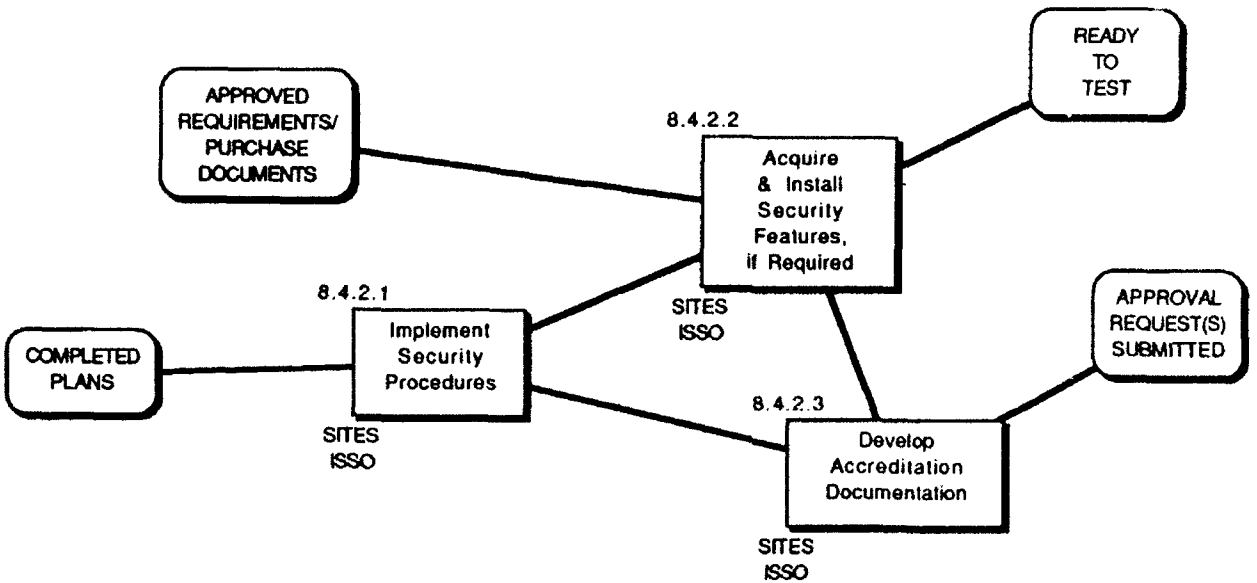
DEVELOP SITE INSTALLATION & INTEGRATION PLANS (8.3)

Figure F-15



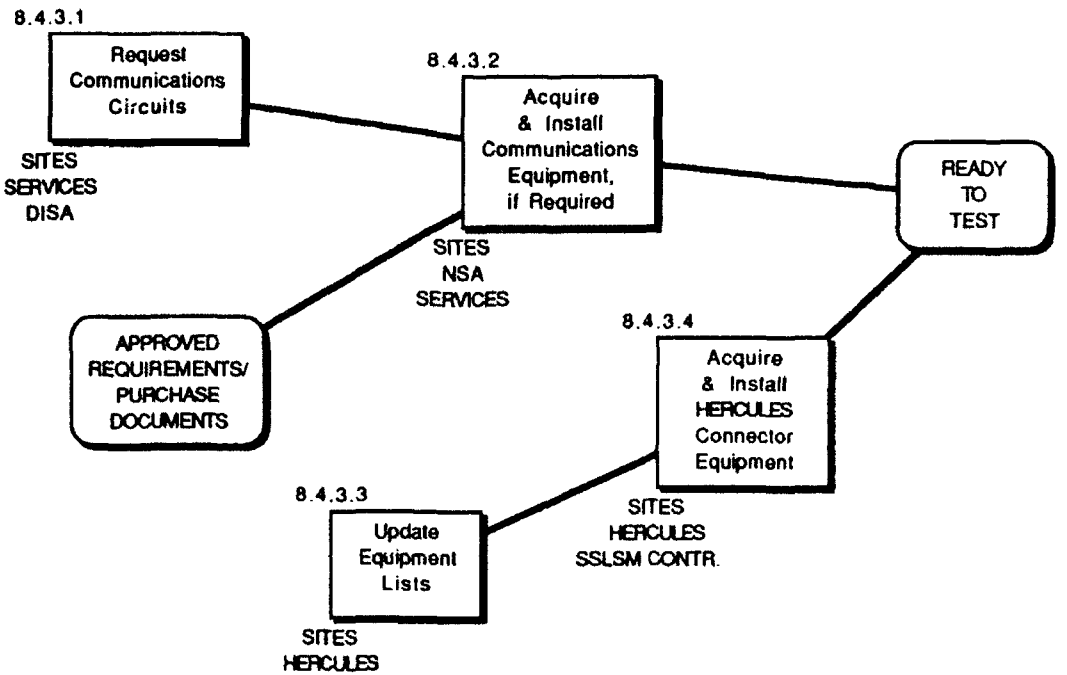
INSTALL & INTEGRATE SITE CM/RD CAPABILITY (8.4)

Figure F-16



IMPLEMENT SITE SECURITY CHANGES (8.4.2)

Figure F-17



IMPLEMENT SITE COMMUNICATIONS CHANGES (8.4.3)

Figure F-18

MISSION

OF

ROME LABORATORY

Rome Laboratory plans and executes an interdisciplinary program in research, development, test, and technology transition in support of Air Force Command, Control, Communications and Intelligence (C^3I) activities for all Air Force platforms. It also executes selected acquisition programs in several areas of expertise. Technical and engineering support within areas of competence is provided to ESD Program Offices (POs) and other ESD elements to perform effective acquisition of C^3I systems. In addition, Rome Laboratory's technology supports other AFSC Product Divisions, the Air Force user community, and other DOD and non-DOD agencies. Rome Laboratory maintains technical competence and research programs in areas including, but not limited to, communications, command and control, battle management, intelligence information processing, computational sciences and software producibility, wide area surveillance/sensors, signal processing, solid state sciences, photonics, electromagnetic technology, superconductivity, and electronic reliability/maintainability and testability.